FOREWORD

The February 2006 revision (Change 6) of the Corporate Examiner's Guide (CEG) consists of an update to Chapters 102, 303, 304 and 401. Change 6 includes revisions to the Information Systems and Technology (Chapter 303) and Item Processing Service Centers (Chapter 304) chapters resulting from technological and regulatory changes, as well as general updating of the other aforementioned chapters and certain associated appendices.

As a reminder to those utilizing this manual the CEG remains a guide, not a regulation. The guidance herein is dependable, but may not be the best or final approach in every situation. Examiner judgment and flexibility remain crucial to a successful examination program.

Kent D. Buckham
Director
Office of Corporate Credit Unions

TABLE OF CONTENTS

OTHER EXAMINATION AREAS 300

ASSESSMENT OF CORPORATE CREDIT UNIONS 400

WORKPAPERS

Chapter 102

CORPORATE CREDIT UNION SUPERVISION AND EXAMINATION PROCESS

Introduction

The Office of Corporate Credit Unions (OCCU) fulfills its mission by promoting and ensuring the safety and soundness of the Corporate Credit Union System (System) principally through a program of continual supervision. Supervision includes, but is not limited to, the on-site examination of corporate credit unions (corporates) resulting in an examination report. Supervision entails vigilance encompassing all regulatory efforts to formulate, implement, and maintain an ongoing process to ensure that:

1. Corporates report their condition in a timely and comprehensive manner;
2. OCCU evaluates and reports the condition of corporates;
3. Corporates correct deficiencies in a timely manner; and
4. The System remains safe and sound.

OCCU's Supervision Goal

OCCU's overall supervision goal is to ensure the safety and soundness of the System by (1) continuously evaluating and supervising the financial condition and performance of individual corporates and their service organizations, and (2) reporting those conditions to the NCUA Board in a timely manner. OCCU provides high-quality "targeted" supervision. The key element in accomplishing OCCU's goal is the timely identification and resolution of any problem or condition that may have a material impact on a corporate, the System, or the National Credit Union Share Insurance Fund (NCUSIF).

OCCU's efforts are focused on (1) identifying existing and/or emerging material problems in individual corporates and/or the System, and (2) ensuring such problems are corrected in a timely and appropriate manner. Since accepting risk is inherent to the business of the System, OCCU's philosophy is centered on evaluating risk.

OCCU applies this philosophy in all its supervisory activities. OCCU combines the structure of consistent supervision with reasoned flexibility to ensure its procedures are appropriate for both the corporate and the dynamic, evolving marketplace in which it operates. Flexibility allows examiners to adjust the supervisory effort to meet the risks posed by a particular corporate while ensuring risks are addressed throughout the System.

Elements of the Supervision Process

Regardless of the approach taken, effective supervision includes, at a minimum, the following elements:

1. Performing high quality annual examinations of all corporates that accept deposits from any federally insured credit union, whether federal or state chartered;
2. Conducting periodic or continuous on-site reviews of corporate activities based on the degree of existing or perceived risk they undertake;
3. Conducting monthly off-site reviews of corporate activities through review of financial and management reports including operating budgets and strategic plans; and
4. Conducting monthly reviews of corporate financial data (NCUA 5310 reports) to determine trends in individual corporates and the System.

In conjunction with its efforts to implement these four elements, OCCU communicates with State Supervisory Authorities (SSA) to coordinate an overall supervision plan. Agreements with SSAs are contained in Chapter 104 and may be supplemented by special agreements with individual SSAs. Examiners should familiarize themselves with any agreements prior to initiating a contact with the SSA to discuss supervision and examinations plans.

Targeted Risk Approach

OCCU employs targeted risk procedures to ensure the examination scope appropriately focuses resources toward areas of material risk. While all areas of risk are addressed, an appropriate examination plan may utilize one or more of the following techniques:

1. Allocate examination hours based on perceived risk the examination areas pose and the extent and results of prior years review of the area;
2. Prioritize areas for a comprehensive review once every two or three years (depending on risk) unless there is a demonstrable need for more frequent or thorough review; and
3. Use examination procedures that test the quality of managerial supervision of the area, reliability of the area's internal controls, and the quality of oversight provided by the board of directors and its auditors.

Targeting risk requires examiners to determine how existing or emerging situations confronting a corporate, or the credit union industry, affect the nature and extent of risks in that institution. The examiner then structures supervisory plans and actions based on the corporate's risk profile. The Targeted Risk approach provides flexibility for the examiner to prioritize the use of resources toward the areas of greatest risk. It officially sanctions the ability and elevates the responsibility of the examiner-in-charge (EIC) to prioritize procedures for resource maximization.

OCCU recognizes corporates must take risks to earn a return. Risk levels, however, must be appropriately identified, measured, monitored, reported, and controlled. The significance of risks must be continually evaluated.

Corporate management is responsible for controlling risk. OCCU assesses how well a corporate manages risk over time, rather than at a single point in time. Targeted risk procedures focus on the oversight rather than an audit role. Targeted risk allows OCCU to concentrate on systemic risks and institutions that pose the greatest risk to the System and the NCUSIF.

OCCU's targeted risk approach identifies areas that, in the aggregate, pose the potential for presenting an unacceptable level of risk to the System and the NCUSIF. To address high-risk activities that can be influenced by market conditions, OCCU's goal is to communicate with, and influence, the System through direct supervision, policy, and NCUA regulation. In situations where corporates are not properly managing risks, OCCU uses appropriate means to influence management to adjust its practices to conform with sound business practices.

Inherent Risks

Some risks are inherent to the System. A wide body of knowledge exists within the System on how to identify, measure, monitor, report, and control these inherent risks. Targeted risk acknowledges these inherent risks and evaluates whether they are properly managed. Other risks in the System are more diverse and complex. These more sophisticated risks require enhanced controls and monitoring by both the corporate and OCCU. OCCU is committed to focusing its resources on these complex and evolving risks, especially when they present material actual or potential risks to the System.

Supervisory Response to Degree of Risk Exposure

Risks that large corporates assume are generally diverse and complex and warrant a targeted risk approach. Under this approach, examiners do not attempt to eliminate appropriate risk-taking, but rather ensure corporates understand and control the levels and types of risk they assume. In situations where risk is not properly managed, OCCU will direct management to take corrective action so the corporate is managed in a safe and sound manner. In all cases, OCCU's supervisory focus is to determine that management identifies, measures, monitors, reports, and controls risks to ensure sufficient capital is present in relation to the corporate's risk activities.

"Pass-through" corporates (those which primarily rely on another corporate for investment placement and product offerings) are generally less diverse and complex than those which deal directly in the financial marketplace. Regardless of each corporate's complexity, the targeted risk approach still emphasizes that all risks be adequately managed.

Targeted Risk Approach

The Corporate Examiner's Guide stratifies targeted risk within base, standard, and expanded examination procedures as discussed in Chapter 101.

A crucial element of the targeted risk approach is the EIC's pre-examination risk assessment of the corporate. (The framework for this process is described in Appendix 102A entitled "Application of the Targeted Risk Approach in the Identification, Measurement, and Assessment of Risk.") During this assessment, the EIC determines and documents the level of supervisory concern for each risk category. Having prioritized the corporate's risk exposure, the EIC selects and documents a detailed examination scope. A determination not to use the standard examination scope will be documented. Advance Corporate Field Supervisor (CFS) approval is required for using anything other than the standard examination scope. While implementing the examination scope as part of the on-site field work, the EIC may determine expanded or base review procedures are more appropriate. These situations should be discussed with the CFS before the examination scope is adjusted.

Targeted Risk Summary

The Targeted Risk approach allocates greater resources to those areas with higher risks. OCCU accomplishes this by:

1. Identifying risks using common definitions. This set of risks forms the basis for supervisory assessments and actions;
2. Measuring risk based on common evaluation factors. Risk measurement is not always quantified in dollar terms; it is sometimes a relative assessment of exposure. For example, numerous internal control deficiencies may indicate a corporate has an excessive amount of transaction risk;

3. Evaluating risk management to determine if the corporate's systems adequately manage and control risk levels. System sophistication will vary based on the level of risk present and the size and/or complexity of the institution;
4. Assigning greater resources to areas of higher or increasing risk, both within an individual institution and among corporates in general; and
5. Performing examinations based on risks, reaching conclusions on risk profile and condition, and following up on areas of concern.

To accomplish these tasks, examiners will discuss preliminary conclusions with corporate management and adjust conclusions and strategies based on these discussions, as appropriate. OCCU can then target supervisory efforts on significant risks.

The targeted risk approach provides OCCU and the System with:

1. A high level of consistency in supervision by using minimum core procedures;
2. An allocation of resources based on risk;
3. Sufficient flexibility to allow examiners to tailor the supervisory effort to the risks present;
4. Less supervisory review of low risk areas; and
5. Help in determining the sufficiency of each corporate's capital level and risk management system.

Planning

Examination/supervision planning is the process of identifying and establishing supervisory goals and objectives for incorporation into OCCU's supervisory strategy for each corporate. On-site examinations, supplemented by on- and off-site supervision activities, are the means by which OCCU's supervisory strategies are implemented and its supervisory goals and objectives are achieved.

The targeted risk approach ensures that OCCU's resources are efficiently used by establishing appropriate examination procedures, and developing appropriate guidelines for OCCU personnel to follow when completing assignments.

Examination/Supervision Planning

OCCU's supervision policies require a specific supervisory strategy for each corporate. The strategy includes detailed, planned supervisory activities. Planning normally begins at the conclusion of a full-scope, on-site examination with the completion of the one-year supervision plan (OYSP). Reference should be made to Appendix 102C for OCCU's format and content requirements for OYSPs and additional discussion in the section below (Developing an Examination/Supervision Plan).

On-going Modification of Examination/Supervision Plans

Examiners perform ongoing supervision and periodic follow-up activities throughout a supervision cycle to identify and assess risks and changing conditions. As supervisory strategy is dynamic, EICs and CFSs should review examination/supervision strategies and revise or update them to reflect the corporate's changing risk profiles, developments in the System, and regulatory changes. Examiners should discuss any approved changes to examination/supervision plans with corporate management.

Developing an Examination/Supervision Plan

Examination/supervision of individual corporates is tailored to conditions and needs according to OCCU policy. This approach balances consistency with flexibility. Annual examination/supervision plans for each corporate are developed as follows:

1. Budget - In conjunction with preparing OCCU's budget, each CFS will recommend to the OCCU Director (Director), the category Type of supervision (discussed below) planned for each corporate during the next examination cycle. The CFS consults with examiner staff before making a recommendation. The Director approves the type of supervision recommended (i.e., assuming agreement with the recommendation), subject to NCUA Board budget approval;
2. OYSP - After each annual examination, the CFS and the EIC will develop the corporate's supervision and examination scope for the forthcoming year. The OYSP addresses what needs to be

accomplished and outlines the most efficient and effective method for achieving the goals established in the OYSP. This includes use of base, standard, and expanded examination procedures (Chapter 101). The plan should also include any on-site visits to monitor operational changes (e.g., software, key staff, new initiatives, and conversions.) The OYSP will be submitted to the Director for approval; and

3. The CFS and the EIC will monitor implementation of the plan on an ongoing basis, notifying the Director of any needed changes/revisions.

Supervision Types

Based on the criteria listed below, each corporate is assigned a supervision type category. The supervision type of each corporate is a key component of the target risk supervision approach and provides standard on- and off-site supervision strategies, based on each corporate's established supervision type. OCCU staff may vary from the supervision strategies for each type if approved by their CFS and the Director.

A corporate's assigned supervision type is not a rigid function of asset size, expanded authority level, or Corporate Risk Information System (CRIS) rating. Rather, it represents a combination of factors that may include these elements in addition to perceived risk levels, quality of or changes in management, financial condition, trends, etc.

Type I

Type I corporates do not have expanded authorities above the Base Plus level.

Supervision of Type I corporates includes:

1. Monthly off-site monitoring by the EIC.
2. Ongoing monitoring of NCUA 5310 report data and trends, as well as monthly verification of data by the EIC.
3. Examination and on-site supervision:

    a. Risk Management and Financial Risk rated either 1 or 2:

1) Annual Examination

b. Risk Management and/or Financial Risk rated no worse than a 3:

1) Annual Examination
2) Semiannual on-site follow-up contact

c. Risk Management or Financial Risk rated 4:

1) Annual Examination
2) Semiannual Examination
3) Quarterly on-site follow-up contact

d. Risk Management and Financial Risk rated 4:

1) Annual Examination
2) Semiannual Examination
3) Monthly on-site follow-up contact

Type II

To qualify for Type II supervision, corporates must generally exceed $1 billion in assets, and/or have expanded authorities above the Base Plus level and exercise its approved powers in a significant and assertive manner. Additionally, Type II corporates have complex and innovative operations, and/or have significant impact in the marketplace, and/or present unusual or unique examination and supervision problems that cannot be adequately addressed by Type I supervision.

Supervision of Type II corporates includes:

1. Monthly off-site monitoring by the EIC.
2. Ongoing monitoring of NCUA 5310 reports, as well as monthly verification of data by the EIC.
3. Examination and on-site supervision:

a. Risk Management and Financial Risk rated either 1 or 2:

1) Annual Examination
2) Monthly one or two week on-site contact by EIC

b. Risk Management and/or Financial Condition rated no worse than 3:

1) Annual Examination
2) Semiannual follow-up Examination
3) Monthly one or two week on-site contact by EIC

c. Risk Management rated 4 and Financial Risk rated 3:

1) Annual Examination
2) Semiannual Examination
3) Monthly two week on-site contact by EIC

d. Risk Management rated 3 and Financial Risk rated 4:

1) Annual Examination
2) Semiannual Examination
3) Monthly two week on-site contact by EIC
4) Weekly review of financial deficiencies

e. Risk Management and Financial Risk rated 4:

1) Annual Examination
2) Semiannual Examination
3) Full time, on-site presence

Type III

Corporates which qualify for Type III supervision, generally, have billions of dollars in assets, and/or have expanded powers in excess of Part I and exercise their approved powers in a significant and assertive manner. Additionally, Type III corporates have complex and innovative operations, and/or have a significant impact in the marketplace and on the corporate and/or credit union system, and/or present unusual or unique examination and supervision problems, which cannot be adequately addressed by Type I or Type II supervision.

Supervision of Type III corporates includes:

1. Monthly off-site monitoring by the EIC.
2. Ongoing monitoring of NCUA 5310 report data and trends, as well as monthly verification of data by the EIC.
3. Examination and on-site supervision - regardless of Risk Management and Financial Risk ratings:

    a. Incremental annual examination, scoped with two separate contacts (i.e., typically investment and ALM phase and an operational risk phase)
    b. Full time presence by on-site examiner, not necessarily the EIC
    c. Monthly on-site EIC contact

For incremental examinations, the CRIS ratings are normally assigned after the operational examination phase. However, OCCU staff has the flexibility to adjust CRIS ratings after any examination phase. These situations should be discussed with the CFS, and if appropriate, the OCCU Director.

Examinations

Scheduling Examinations

Annual examinations are required and performed for all corporates. On-site follow-up examinations and supervisory contacts are performed consistent with the corporate’s supervision category. Appendix 102B provides a timeline for completion of examination related activities.

Examination Teams

Examinations are performed by teams, composed of an EIC and one or more team members. The EIC and team members are assigned by the CFS based on a variety of factors such as corporate complexity, examiner experience, examiner proximity to the corporate, and scheduling considerations. Appendix 102F, Reduced On-Site Examinations (ROSE) also impacts examination team planning.

Examination Steps

An examination entails a number of steps in planning and execution. These steps generally include:

1. Off-site pre-examination planning;
2. On-site pre-examination preparation;
3. Examination field work;
4. Exit briefing;
5. Report writing;
6. Joint conference; and
7. Wrap-up.

Pre-Examination Planning

Prior to each examination, the EIC has responsibility to plan the on-site (field) examination work. This planning effort is accomplished during a period referred to as pre-examination. The pre-examination effort may be accomplished both on- and off-site, by the EIC.

By necessity, pre-examination planning is conducted approximately 45 - 60 days in advance of the examination, and generally requires from three days to one week to complete. Pre-examination planning is an opportunity for the EIC to:

1. Make team participant lodging arrangements;
2. Arrange for corporate management to complete and return to the EIC, the Pre-Examination Questionnaire (OCCU 102Q);
3. Develop the preliminary examination scope and time budget;
4. Prepare a memorandum to team participants regarding their participation on the examination; and
5. Prepare a letter to the corporate being examined to communicate the dates of the on-site examination, the exit and joint conference dates and times, to provide them with the information request list, and to request arrangement for review of the annual audit work papers.

Factors to consider in the pre-examination planning process:

1. Attain goals and objectives - The examination effort should be directed toward attaining the supervisory goals and objectives that were previously identified and established during the examination/supervision planning process. (e.g., OYSP, pre-examination questionnaire, monthly management reports.)
2. Develop scope - Examination procedures contained in the individual programs are designed to be comprehensive and target risk areas. Therefore, it is important appropriate procedures are selected within each program.
3. Plan for optimum productivity - The EIC should plan opportunities for meetings with examination staff and corporate personnel, arrange adequate workspace for the examination team, and prioritize and schedule workflow.
4. Make assignments and monitor job - The EIC must determine the expertise necessary to perform certain aspects of the examination and make assignments accordingly. When assigning more than one individual to an area, it is recommended that a team leader be assigned who will be responsible for its completion. Training and development needs should also be considered when making examination assignments.
5. Budget and monitor overall time - The EIC must consider the time budget when assigning tasks. A useful tool for improved personnel planning is a time and planning summary organized according to sections of the examination. Such a summary specifies areas for which procedures are planned and provides a comparison of actual and budgeted hours. As the examination progresses, the time budget should be modified as deemed appropriate.
6. Assign priorities - The EIC assigns priorities to each area. Ordinarily this can be accomplished by assigning related areas to one team leader who subsequently coordinates the work of others.
7. Schedule examination - To minimize costs and disruption to the corporate, it is important that the examination be conducted as quickly as practical. It is the responsibility of the EIC to discuss any planning problems with the CFS. If corporate management is concerned about scheduling, this matter should also be discussed.

Pre-Examination Questionnaire (OCCU 102Q)

This questionnaire contains questions detailing the nature and complexity of the corporate’s operations and internal controls. It is designed to assist the EIC in planning examination procedures and resources. It should be completed as one of the first steps of the Pre-Examination planning effort. Ideally, it should be prepared by corporate management or by the EIC during an interview with corporate management. Any questions not answered affirmatively should be explained in the comment section of the questionnaire and/or in the appropriate CEM by the examiner responsible for that area.

On-Site Pre-Examination Preparation

Examiners utilize on-site examination preparation time to accomplish several purposes:

1. Review the Pre-Examination Questionnaire which management has completed at the EIC’s request and make any necessary changes in the preliminary scope;
2. Ensure management provides the items listed in the information request list so they will be available when the examination team arrives;
3. Ensure adequate work space is available for the team; and
4. Review the work papers supporting the annual audit.

On-site examination preparation efforts are generally performed during the first few days of the week preceding the on-site arrival of the examination team (first day of examination field work). This timing allows the EIC to review information provided by management pursuant to the pre-examination request, make any necessary changes in the preliminary scope, and follow-up on any requested information management has yet to make available.

Examination Field Work

Depending on the size and complexity of the corporate, an examination usually entails two to three weeks of on-site field work. The duration of a Type III incremental examination may vary.

During this period, the examination team gathers information and performs procedures as outlined in the examination scope.

<u>Managing An Examination</u>

Managing an examination is as important as planning it. The level and sophistication of management methods and procedures varies depending on the activities to be performed and the size and nature of the corporate. The EIC carries the responsibility for managing the examination.

Inherent in the EIC's responsibilities is ensuring supervisory objectives are met and activities are completed timely. To accomplish these goals, the EIC must continually monitor the progress of the examination, supervising, coordinating, and evaluating the work flow.

Key elements the EIC should consider during the course of the examination are:

1. Communicate examination objectives – The EIC must ensure that examiners understand the objectives of the examination and their assigned programs. Examiners should notify the EIC as questions occur regarding scope or depth of review. Examiners should not vary from standard examination procedures unless the EIC determines that such procedures are necessary to address potential risks. Ongoing communication between the EIC and team participants is critical to effective examination management;
2. Monitor staff performance - Examiners' performance must be monitored throughout the examination to ensure objectives are being met according to schedule and to prevent problems from developing. It is also important to avoid material deviations from the examination scope into unplanned activities. Early identification of work-related problems also allows examiners the opportunity to correct mistakes and to immediately improve skills;
3. Monitor the examination - Monitoring the examination's progress allows early adjustments to the scope, staffing, and completion

date, as necessary. The EIC must notify the CFS if examination scope adjustments are necessary;

4. Training and evaluating examiners - Examiners may frequently need guidance, depending on their experience and ability. Questions should be encouraged and the EIC is responsible to ensure someone is available to provide guidance;
5. Communicate effectively - The EIC must maintain effective communications with the CFS, corporate management, the SSA, and examiners regarding the examination's progress;
6. Complete work papers - Prepare, file, index, and review work papers to facilitate efficient preparation of the examination report; and
7. Out-brief examiners - The out-briefing process is critical to the conclusion of the on-site examination effort. As the field work draws to a close, the EIC must have a complete understanding of the work performed and issues identified by each team member. Ideally, the EIC will monitor all team members' activities during the examination so the out-briefing is minimal. The out-briefing should provide an orderly transfer of examination materials, such as work papers, reference material, time sheets, etc., from the participant to the EIC or the EIC's designee. The EIC should also be informed of any additional items requested during the examination that should be added to the request list for the next examination.

Work Paper Documentation

Integral to the targeted risk approach is its system of work papers designed to assist the EIC in examination planning, coordinating, observing, understanding, critiquing, reporting, and follow-up. Overall, examination work papers provide efficient vehicles for the examiner to report both the understanding obtained and concerns identified.

Required work papers for each examination include:

1. A Corp110 form identifying the ratios, CRIS ratings, time spent, and problem areas;
2. National Credit Union Administration Examination Report, OCCU 102B and OCCU 102C - These forms are the standard report letter

page for the distribution of an examination report. OCCU 102B is utilized for a report to a federally chartered corporate credit union and OCCU 102C is used for a state chartered corporate credit union. These forms list the procedures used during and objectives of the examination, cite the responsibility of the board of directors and management, and provide instructions on how to address the report's findings;

3. Executive Summary, OCCU 102D - The Executive Summary summarizes the examiner's review, analysis, and findings in major areas of the corporate's operation, financial condition, management, and CRIS ratings;
4. Supplementary Facts, OCCU 102E - The Supplementary Facts is used to discuss material facts or situations not contained in other narrative sections of the examination report or to expand on Executive Summary discussions. This form is optional;
5. Document of Resolution (DOR), OCCU 102F - This form is designed to record and report the findings, issues, and actions needed to correct findings for issues of major importance. Matters presented on this form must represent violations of law, regulation, policy, and/or must constitute a material safety and soundness issue. As OCCU 102F issues are identified, examiners should:

   a) Confirm their understanding of the facts and circumstances surrounding the issue and the corresponding basis for the exception;
   b) Prepare the OCCU 102F; and
   c) Report the finding and provide a copy of the OCCU 102F to the team leader (if any) and the EIC.

   The EIC should seek management's agreement for action plans, responsible parties, and the time frame for resolving DOR issues. However, sometimes management's time frame may be inadequate to bring out regulatory compliance or adequate management of risks. Nevertheless, due dates should be reasonable and attainable and due dates not met will require additional correspondence between the OCCU/SSA and the corporate. OCCU/SSA must officially approve all due date changes after the final report is presented;
6. Other Examiner's Findings (OEF), OCCU 102G - The examiner has broad latitude regarding the documentation of issues, which do

not merit inclusion on the OCCU 102F. The OCCU 102G has been devised to serve as a vehicle to report issues about which the examiner has a concern, but which are not material and are not appropriate for inclusion on the OCCU 102F.

OCCU 102G issues should be discussed with departmental management as they are identified during the examination. This form will be provided to the corporate's directors no later than the conclusion of the joint conference. Normally, it will not be included in the official examination report. However, with the concurrence of the CFS, the examiner may include the form with the report if the number of non-material items, when considered as a whole, will have a material impact on the overall evaluation of any component of either the financial risk or risk management rating. When it is included as a part of the report, the examiner will explain the reasons to the corporate's board. The Executive Summary will detail to the officials whether this form is included in the examination report or handed out separately;

7. Trends on the Consolidated Balance Sheet Report (CBS, a product of the 5310 System) – The CBS is generated and analyzed during each examination and it, or a similar financial trend work paper is included in the examination report. The CBS provides monthly balance sheet, income, and ratio trends;
8. Procedures and Questionnaires - These forms are developed as part of the examiner's review responsibilities. The examiner should ensure that adequate comments are made as appropriate. The comment should be descriptive enough for a reviewer to draw a conclusion. Repetitive comments in the examination procedures, questionnaires, or Corporate Examiner Memorandums (CEM) should be avoided or at least minimized;
9. CEM, OCCU 102H - This form is developed as part of the examiner's Observation/Reviewing responsibilities. The examiner develops a thorough understanding of assigned processes as they are uniquely implemented in the corporate being examined.

   OCCU 102H should be a professionally written document that outlines the review area. The document should not contain non-verified information or hearsay. The document is presented to the corporate for accuracy and verification of the examiner's understanding of the policies, procedures, and practices. OCCU

102H is designed to be carried forward from year to year and updated/revised only as necessary to reflect any changes to the operation that have been made since the prior examination. Concluding each OCCU 102H is a brief narrative overview summarizing the examiner's conclusions regarding the operational status of the area reviewed. This should be a conclusions-reached memorandum - not a listing of the review steps the examiner accomplished;

10. CRIS, OCCU 102I - This form is used to support the CRIS ratings (See Chapter 401) assigned by examiners during the examination. From this form, the EIC will derive the composite and component CRIS ratings which will be included in the Executive Summary, OCCU 102D. The SSA may have a separate rating or may use the CAMEL rating system for state chartered corporates;
11. Confidential Section, OCCU 102J - The Confidential Section is for NCUA's internal use only. However, situations exist when all or part of a report's Confidential Section may be released by court order or in compliance with a Freedom of Information Act request. The possibility of release should not dissuade examiners from presenting necessary information; however, examiners should maintain their professionalism and objectivity when writing the Confidential Section.

    Examiners are to report corrective and constructive work accomplished during the examination in the Confidential Section if not included in the open sections of the report. Examiners should comment briefly but completely enough to clearly reflect actions taken. Of particular importance is an explanation of what the examiner accomplished during discussions with officials and management. If not discussed elsewhere in the report, the Confidential Section should state what formal actions the board took and how the officials will handle major problems. At a minimum, this form should report:

    a. Advanced meetings with management;
    b. Joint conference;
    c. Deviations from scope and budget;
    d. Date of problem code assignment and elimination;
    e. Report distribution;
    f. Transmittal letter dissemination; and

g. Recommended follow up.

Examiners should include in the Confidential Section pertinent matters of a private or restricted nature, including professional opinions based on the examiner’s observations. However, the examiner should not make statements based on gossip or hearsay;

12. Other examiner-designed work papers - Examiners are authorized and encouraged to use their professional judgment in devising unique work papers to supplement core work papers for the assigned area of review. However, excessive documentation should be avoided and such work papers should only include information that is relevant and/or may require follow-up. Time spent recording extraneous information is better spent examining high-risk areas; and
13. Electronic database storage – The final examination report, CEMs, procedures, questionnaires, and custom work papers will be submitted to OCCU mail for electronic filing. All OCCU staff will ensure they abide by all policies and guidelines in maintaining and transmitting sensitive examination information (i.e., use NCUA computers, the VPN, etc.).

Exit Briefing

The exit briefing with corporate officials and management will be held at the conclusion of the examination fieldwork. The EIC must verify that all officials have been invited to attend the exit briefing. It is up to the board members (not operating management) to decide which officials will be in attendance. It is up to the discretion of the EIC what will be discussed during the exit briefing (e.g., DORs, OEFs). The EIC must have sufficient understanding of the issues to proficiently discuss them during the exit briefing.

Report Writing

Depending on the size and complexity of the corporate and/or deficiencies noted during the examination, the EIC is afforded one week to consolidate, review, and analyze the team’s work papers and prepare and submit a draft report for supervisory review. It is expected that the draft report will be a professional product, void of grammatical, punctuation, and spelling errors. The draft report will be sent to the CFS and SSA (if applicable) for review and finalization.

While writing styles will vary, the EIC should ensure the examination report discusses facts, expresses OCCU's assessment of the various risks or issues, and provides closure for the issue at hand.

Joint Conference

The joint conference is usually scheduled as part of the pre-examination planning process. The joint conference should be set to accommodate the corporate, OCCU, and the SSA. Regularly scheduled board meetings usually work; however, special meetings may need to be called. A visual aide must be used for each joint conference. This could include power point, flip charts, handouts, etc. The joint conference must be a professional meeting held to summarize the financial condition of the corporate and examination findings. The ratings of the corporate will not be disclosed until the end of the joint conference.

OCCU attendees at the joint conferences are normally provided advance notification via an information memorandum developed by the EIC. A sample of this memorandum is shown in Appendix 102D.

Wrap-Up

After the joint conference the EIC will finalize the examination work papers and necessary forms. This includes:

1. Finalizing the confidential section;
2. Finalizing the transmittal letter to the corporate, region memorandum (see Appendix 102E), and SSA memorandum;
3. Preparing a OYSP per this chapter and OCCU Instruction 9600, including establishing the scope for the next 12 months supervision;
4. Sending a zipped copy of the database to OCCU;
5. Uploading the Corp110;
6. Sending work papers to OCCU, CFS, and SSA (if requested); and
7. Updating all other forms/logs required by OCCU (e.g., CUSO Logs, Privacy Checklist), if applicable.

Supervision

On-Site and Off-Site Supervision Process

Corporates are an integral part of the System and the credit union industry. Additionally, they have the ability to take risks in the management of their assets as they provide services to their members. Due to the complexity and inherent importance of corporates, on-going supervision is needed to ensure the safety and soundness of individual corporates and the System. Effective and continuous review of a corporate's operations is an essential part of the supervision process.

Files

EICs maintain field files for each corporate in their district. These files should include not only documents, analysis, and reports related to previous examinations and supervision contacts, but also current policies and procedures for all critical areas of operation. The files should be well organized to ensure their efficient use and, when necessary, their orderly transfer to other OCCU staff. It is imperative that hard and electronic examination information be formally and safely maintained and transferred. The following minimum information should be maintained:

1. Permanent file (containing a history of examination reports, regulatory information, critical correspondence, etc.);
2. The last one or two complete examination work papers;
3. Supervision contacts during the examination period;
4. Board and ALCO packages for the examination period;
5. Current budget and strategic plan;
6. Examination period correspondence; and
7. Monthly management reports, 5310s, and Corp110s.

Information Received

To supplement the files maintained, each EIC will receive monthly board and ALCO packages from corporates in their district. The packages, at a minimum, should include the following:

1. Monthly board and committee minutes with supplemental attachments (e.g., proposed policies, individual new product business plans, status of DOR and OEFs);
2. ALM reports (e.g., NEV, spread analyses, and book of business);
3. Financial statements, including a delinquent loan report;
4. Audit and internal control reviews completed;
5. Budget comparisons; and
6. Current lists of investments and new investments purchased during the month.

The examiner must verify DORs are completed within the agreed upon due dates. The examiner will initiate necessary correspondence, which includes correspondence from the Director and SSA (if state chartered), if due dates will not or have not been met. The areas of concern within a DOR must be monitored and reported as noted in NCUA Instruction OCCU: 4000.02 entitled *Problem Area Resolution* dated January 6, 2005.

Analyses Performed

While conducting on-site and off-site supervision contacts, the EIC will perform, at a minimum, specific supervision functions. The following supervision tasks are key to determining whether an immediate on-site contact is required, the current on-site contact is expanded, and the scope of the next examination or supervision contact.

1. Analyze financial trends;
2. Ensure timely compliance with the previous examination report's DOR and OEF;
3. Assess management changes (e.g., board of directors, senior management, and other key employees);
4. Assess changes to MIS systems or major related systems (e.g., item processing);
5. Monitor and analyze changes in the investment portfolio and ALM strategies;
6. Review and verify for accuracy financial information submitted monthly by corporates, via the 5310 system; and

7. Review all material changes in policies, procedures, practices, and operations.

Other On-site Supervision Contacts

Other situations could warrant an on-site contact. This could be completed by the district examiner or with a team of examiners. The following situations could warrant an on-site contact:

1. CRIS rating - to follow-up on the status of completing DORs and correcting OEFs;
2. Expanded Authority Request (EAR) - to evaluate the EAR and prepare for the OCCU Director and/or NCUA board action and SSA concurrence, if required;
3. Request for NCUA board action - to evaluate the corporate's request and prepare for the board action;
4. Senior management change - a change in senior management could warrant a contact to verify accuracy of reports and overall condition of the corporate; and
5. Addition or deletion of a service - a purchase or sale of a service or a fixed asset that could have a material impact on the membership.

In all situations, the examiner should prepare appropriate documents supporting the contact. This could include a contact memorandum documenting work performed, status reports for DORs and OEFs, and appropriate documents for requested actions.

If appropriate, CRIS ratings can be reevaluated during a supervision contact. Ratings will be changed, as deemed appropriate, based on favorable/deteriorating financial, managerial, and/or operational factors. OCCU reserves the right to change CRIS ratings, as warranted, with the concurrence of the OCCU Director.

Examination Objectives

Examination Planning and Control Objectives

1. Prepare for supervisory activities, including the on-site examination, in an efficient manner;
2. Select and structure examination programs that target the goals and objectives of the supervisory strategy;

3. Ensure the examination is conducted in a professional manner;
4. Establish controls and record keeping systems to communicate examination findings effectively; and
5. Maintain review processes to ensure prescribed work is completed and workpapers support conclusions.

Supervision Contact Objectives

Objectives of both on- and off-site supervision contacts

1. Obtain reasonable assurances each corporate will continue to be financially sound;
2. Determine NCUSIF risk;
3. Determine compliance with applicable laws and regulations; and
4. Determine that the corporate's activities and financial condition does not adversely affect the System.

Examination Procedures

See Corporate Examination Procedures - Examination Administration (OCCU 102P).

Examination Questionnaire

See Pre-Examination Questionnaire (OCCU 102Q).

Appendices

102A – Application of the Targeted Risk Approach in the Identification, Measurement and Assessment of Risk

102B - Examiner's Guideline for Completing an Examination

102C - Template for the One-Year Supervision Plan

102D – Template of Joint Conference Information Memorandum

102E – Sample Transmittal Memo to the Region

102F – Reduced On-Site Examinations

APPENDIX 102C
Template for the One-Year Supervision Plan

NATIONAL CREDIT UNION ADMINISTRATION
Office of Corporate Credit Unions

OCCU/
CU #

TO: Director
Office of Corporate Credit Unions

FROM: Corporate Examiner
Corporate Field Supervisor

SUBJ: One-Year Supervision Plan (OYSP): Corporate Name, Charter/Insurance Number

DATE:

BACKGROUND

Discuss examination, financial information, areas of concern, etc.

CRIS RATINGS

Financial Risk	**Rating**	**Trend***	**Risk Management**	**Rating**	**Trend***
Empirical Capital			Capital Accumulation Planning		
Earnings			Profit Planning & Control		
Interest Rate Risk			Interest Rate Risk Management		
Liquidity Risk			Liquidity Risk Management		
Credit Risk			Credit Risk Management		
			Operations Risk		
			Board Oversight, Audit and Compliance		
Financial Risk Composite			**Risk Management Composite**		

***Use + for positive trend, – for negative trend, and = for stable.**

CHANGES IN OPERATIONS

Discuss new initiatives, business plans, strategy, management, and information systems changes affecting future supervision plans and/or the focus of the next annual examination. Discuss financial risk, the quality of risk management, the aggregate risk, and the direction of the risk. Any material negative change in direction of risk must be discussed.

APPENDIX 102C
Template for the One-Year Supervision Plan

SUPERVISION TYPE

Discuss supervision type and parameters as outlined in Chapter 102 of the Examiners Guide.

SUPERVISION PLANS

Monthly/Ongoing	OnSite
1.	1.
2.	2.
3.	3.
4.	4.
5.	5.

Discuss any foreseeable changes that could alter the supervision plans. It is not necessary to repeat the discussion of any issues previously covered in the operational changes section on page one.

ANNUAL EXAMINATION

Discuss the next year's annual examination e.g., staffing, budget hours, additional expertise requested. Please note in the table below whether OCMP, CMS, ISS, or PSS participation is requested. Involvement of specialists should consider the risk profile, and should directly relate to the resources necessary to accomplish the supervision and examination strategy.

You need to ensure you document if an area did not receive a comprehensive review and when one is expected. Discuss whether base or expanded procedures were used on any focused area and what is anticipated for the next annual examination. The EIC needs to ensure a comprehensive review (at least standard procedures) of each area is completed every 3 years or more frequently, if necessary.

NEXT YEAR'S RESOURCES REQUESTED TABLE

RESOURCES	# HOURS REQUESTED BY EIC	# HOURS APPROVED BY CFS
CMS		
PSS		
ISS		
OCMP		
CEs		
Other		
Totals		

APPENDIX 102C
Template for the One-Year Supervision Plan

QUESTIONS FOR SPECIALIST PARTICIPATION

Attached is a spreadsheet which will help the EIC determine if a specialist is required. Note: There are three tabs inside the workbook one for each specialized area.

The spreadsheet must be filled out and submitted with the OYSP. EIC discretion is still required when completing the form. A YES answer may not necessarily mean a specialist is required on the next examination. The EIC must evaluate a YES question relative to the overall risk profile of the corporate. If the EIC has any concerns they should discuss with a specialist and the CFS. This form may be used in the future by OCCU to determine risks/changes globally within corporates.

D:\My Documents\
amydata\OCCU\Planr

COMMENTS

Discuss competitive pressures, key issues going forward, future earnings, operational weaknesses, etc.

CUSOs

If applicable, address whether you recommend a separate CUSO review and provide support for your recommendation.

CONCURRENCE

□ Yes

□ No

____________________ ____________

Kent Buckham Date
Director

Chapter 303

INFORMATION SYSTEMS AND TECHNOLOGY

Introduction

The Information Systems and Technology (IST) program provides information services needed to effectively manage the corporate. Hence, the board of directors and senior management must determine what information is needed to make informed decisions and monitor activities of the corporate. From this point, systems must be developed to ensure that the desired information is usable as performance measurements.

A corporate's IST program should be designed to:

1. enhance communication;
2. deliver complex material throughout the corporate;
3. provide an objective system for recording and aggregating information;
4. provide timely and reliable information for services provided to the membership;
5. reduce expenses related to labor-intensive manual activities;
6. support the organization's strategic goals and directions; and
7. provide effective interface capabilities among separate systems.

The five components listed below are essential in considering the usability of any IST program. Management decisions and strategies may be rendered invalid or detrimental if any one of these components is compromised.

Examiners must review the following components during the examination:

1. Timeliness - Information must be current and available to all appropriate users to facilitate timely decisions. This necessitates prompt collection and editing of data.

2. Accuracy - A sound system of internal controls must be in place to ensure the accuracy of data. Information should be properly edited

and reconciled with the appropriate control mechanisms in place. A comprehensive internal and external audit program would greatly facilitate this endeavor.

3. Consistency - Consistency is needed to ensure data provided is valid, as it is relied upon in making decisions and evaluating strategies. Variations in how data is collected or reported can distort trend analysis. Any change in collection or reporting procedures should be clearly defined, documented, and communicated to all users.

4. Completeness - Information input into IST must be complete.

5. Relevance - Information provided must be relevant. Details which are inappropriate, unnecessary, or unsuitable are of no value in effective decision making.

Decision makers cannot fulfill their responsibilities unless all pertinent information is provided in a comprehensive, yet concise format.

Care should be taken to ensure senior management and the board of directors receive relevant information in order to identify and measure potential risks to the corporate. Sound IST procedures are a key component of management effectiveness and should be evaluated in relation to the size, structure, and decision-making process of each individual corporate.

Advances in technology have helped corporates improve both information availability and models for analysis and decision making. Regardless of the technology employed, it is management's responsibility to develop an information system which facilitates the corporate's activities.

An effective IST program draws information from a number of sources for users with various needs. An IST program must selectively update information and coordinate it into meaningful and clear formats. A realistic approach would be to integrate a corporate's accounting system with other resources such as: information regarding economic conditions, characteristics of the market place, competitors, technology, legal/regulatory requirements, et cetera.

Processing Environment

The increasing reliance on automated system technologies by corporates has significantly increased the risk of financial losses due to inaccurate recordkeeping, unauthorized access to financial and members' records, interruption of member service, or fraud. These risks are increased further by the growing use of on-line systems, microcomputers, local area networks, and remote access to records. As a result, the growth of these automated technologies has expanded the scope of IST risk to include all user areas of a corporate.

In general, corporates have a number of choices available to meet their data processing needs. They include: installing an in-house computer center, using a service bureau, or contracting with a facilities management company to manage an existing in-house computer center. Regardless of the type selected, it is essential the board of directors and management establish appropriate policies, procedures, and controls over data processing activities to ensure the accurate processing of information, the privacy of financial and members' records, and the continuation of service in case of disasters.

In-house Computer Center

In-house computer systems vary in size and complexity according to the size of the corporate, the number of applications processed, the transaction volume, and processing deadlines. Computer equipment may vary in size from large "main frame" systems to smaller minicomputers installed as a "turnkey" system. In the turnkey system, a vendor company installs and tests the computer software before the system is turned over to the customer. Software for in-house computer systems may be developed in house or purchased from outside vendors.

Some IST risk areas posed by using an in-house computer system are inadequate hardware and software systems, excessive cost, lack of internal controls, inaccurate financial and customer data, unauthorized access to data processing files, and lack of a disaster contingency plan.

NOTE: The majority of corporates have either an in-house system or minicomputers installed as a "turnkey" system. In most cases, the Corporate Credit Union Network (CCUN) system is the main data system used by corporates. The CCUN system is expected to be replaced in the near future.

Information Security Risk Assessment

Corporates must maintain an ongoing information security risk assessment program that effectively gathers data regarding the technology assets of the organization, threats to those assets, vulnerabilities, existing security controls and processes, and the current security standards, and requirements. The program should analyze the probability and impact associated with the known threats and vulnerabilities to its assets and prioritize the risks present to determine the appropriate level of training, controls, and testing necessary for effective mitigation.

Firewalls

Firewalls are an essential control for a corporate with an Internet connection and provide a means of protection against a variety of attacks. Firewalls should not be relied upon, however, to provide full protection. Corporates should complement firewalls with strong security policies and a range of other controls. Corporates can reduce their vulnerability to attacks somewhat through network configuration and design, sound implementation of its firewall architecture, and intrusion detection systems.

Corporates have a variety of firewall options to choose from depending on the extent of Internet access and the complexity of the network. Based on system complexity, consideration of firewall options should include the ease of firewall administration, degree of firewall monitoring support through automated logging and log analysis, and the capability to provide alerts for abnormal activity.

Intrusion Detection

Corporates should have the capability to detect and respond to an information system intrusion commensurate with the risk tolerance established by the board of directors. Preemptive practices should include the analysis of data flows, decisions on the nature and scope of monitoring, and the development of appropriate policies governing detection and response. The response to an intrusion should include the containment and restoration of systems and appropriate reporting to senior management and officials.

Controls

There are basic controls which must be present in any level of computer operations. These controls should be present at the data center. The evolution of microcomputer-based systems has not eliminated the need for basic controls; rather it has increased the focus of control at the end-user level.

IST controls prevent, detect, correct, and enable recovery from problems that can result from accidents, errors, misuse, sabotage, loss of equipment, loss of data, and any other occurrence that may lead to an unwanted or unexpected disruption of service. The three major categories of IST controls are 1) management controls, 2) general controls, and 3) applications controls.

Management Controls

The reviewer should have a good understanding of how a corporate manages its information systems and services it provides to its members. Similar control issues exist for this area and those generally found in other operational areas, and they require similar review procedures. Good IST management includes:

1. Organization. A corporate should have a well-defined organizational structure that includes the IST department or service area. Ideally, corporates should establish IST as a separate entity that reports directly to management and not through another department. The IST department should maintain an up-to-date topology (a visual representation of the hardware layout) to describe how various systems interact and share data.

2. Planning. The corporate's short- and long-term plans should identify management's direction regarding its IST operation. Management should regularly document, update, and review these plans, which should include well thought out designs for installation of new systems and modification of existing ones.

3. Policies and Procedures. Policies and procedures must be in writing and should define steps to be taken to protect the corporate's computer systems. Management should designate responsibility within the corporate to monitor the acquisition and use of computers. The policy should ensure the required degree of compatibility exists among hardware and software systems throughout the corporate.

4. Monitoring Operations. The crucial oversight function of IST operations can involve the use of committees such as an IST management committee, IST steering committee, or the supervisory committee.

5. Audit. Auditing the IST area is a cost of doing business. Corporates should require regular internal and external reviews of IST operations and services.

General Controls

General control issues exist in any automated environment and remain essential to the day-to-day operation of any IST system. General controls are not specific to any one application or function. General controls should address the following areas:

1. Organizational. The corporate should establish and maintain separation of duties which is a key element of any IST operation. Good internal controls prevent any single employee from having control over the input, processing, and output of transactions. A compensating control, in smaller corporates, could be frequent and detailed review of transaction logs. Other important areas include employment procedures, job descriptions, security statements to help control data, and termination procedures.

2. Data center management. The operation of the data center includes the control and scheduling of input and output, problem prevention and correction, and reporting. Procedures should be in place and up-to-date for each of these areas.

3. Software controls. Corporates must control access to software by unauthorized persons, especially the control and use of the operating system, software utilities, communications, and security software. System logs are useful tools for monitoring activity and changes to the system if management produces and reviews them regularly.

4. Hardware controls. Corporates should document and enforce external controls on hardware including: access controls, terminal usage, and system support and service. Computers have internal hardware controls including: validity, parity, and echo checks that most users do not see. These hardware controls monitor and check for proper hardware function.

5. Physical security. The computer room should have evidence of physical controls including: access controls and logs, fire and theft protection, terminal access controls, and protection of data files and media. Log-on procedures, user IDs, passwords, and physical or electronic keys will provide additional access control to the system.

6. System design, development, modification, testing, and implementation. Corporates should document the methods and procedures for developing and testing new and enhanced systems.

7. Contingency plan. The ability to retain, restart, and replace activity quickly is an important control feature of any IST system. A well-run and controlled operation includes a written and tested contingency plan, proper backup and recovery actions and procedures, and management’s commitment to contingency planning.

Application Controls

Application controls apply to the processing of data into, through, and out of the system. An awareness of IST controls enhances the review of automated parts of the process. A third-party review of this area is recommended in most corporates. Application controls consist of the following:

1. Data origination. Basic controls of data origination include batch totals, control totals, turnaround documents, and retention of source documents. Source documents should be designed for easy and accurate data input.

2. Data input. Controls of data input include conversion, validation, editing, error handling, and separation of duties.

3. Data processing. External controls maintain the operation of the system until completion of the application processing. These controls include system start-up procedures, backup and emergency procedures, error message debugging, and system and job status reporting. Internal validation and editing routines built into the programming checks for errors. The corporate should have error handling procedures to identify and correct transaction errors.

4. Data output. Balancing and reconciliation, distribution, error handling, and records retention procedures complete the application processing function.

Backup and Recovery

Corporates should regularly and routinely backup computer data. Several considerations involving backup and recovery of information include:

1. Frequency. Corporates should backup data files at least daily; application files both when they make changes and routinely, usually monthly or quarterly; a current copy of the operating system, and vital records every three months.

2. Generations. Many corporates keep five sets of data file backups, one made each day of the week.

3. Storage. Corporates must store vital records off-site, at a location far enough from the offices, to avoid the simultaneous loss of both sets of records. Corporates should keep backup files both on- and off-site. Any off-site set of tapes should be encrypted for additional security.

4. Management. Corporates should routinely control, maintain, and test backup files for quality and accuracy.

5. Recovery. Corporates should address and document relevant issues including the speed of data file recovery, who can recover them, and under what conditions.

Contingency Planning

Restoring operations to an acceptable level within a reasonable amount of time requires that all corporates using any type of IST services have a comprehensive, written, accurate, up-to-date, tested contingency plan. Responsibility for developing this plan lies with management of the corporate. Refer to Chapter 307 – Contingency Planning for further information.

Audits

The audits of the IST area, including both internal and external reviews, give the corporate assurance that the system's design and operation function is as intended. Internally, the corporate should perform, at a minimum, quality and accuracy checks on the system's processing to ensure the presence of at least the minimum control requirements for each type of system in use. Depending on the complexity of the IST systems, a corporate may need a complete third-party audit. In addition, external and internal penetration assessments should be performed. Complex corporates may need an internal IST auditor to perform routine, recurring reviews of the system.

Outsourcing

Corporates often rely on third parties to provide and support technology-related functions and services. Outsourcing arrangements can help manage costs, provide expertise, as well as expand and improve services offered to members. Corporate management ultimately remains responsible for managing the risks associated with the system or service.

Corporate management is responsible to ensure member data is protected, even when the data is transmitted, processed, or stored by a third-party provider. Third-party providers should have appropriate security testing based on the risk to the organization. Corporate management is responsible for monitoring the testing performed by the third-party provider through review of timely audits and test results or other evaluations.

Security and Privacy

Part 748 of the NCUA Rules and Regulations requires each federally-insured credit union to develop a written security program. This program must strive to:

- Protect each credit union office from robberies, burglaries, larcenies, and embezzlement;
- Ensure the security and confidentiality of member records, protect against anticipated threats or hazards to the security or integrity of such records, and protect against unauthorized access to or use of such records that could result in substantial harm or serious inconvenience to the member;
- Assist in the identification of persons who commit or attempt such actions and crimes; and
- Prevent destruction of vital records, as defined in 12 CFR Part 749.

The appendix to Part 748 provides guidelines to assist credit unions in meeting the above four criteria. The guidelines provide a good framework from which a corporate credit union can work to develop their policies and procedures.

Security Policies and Procedures

The corporate should consider the following when developing security policies and procedures:

- Identifying the services provided and systems (hardware and software) used;
- Identifying the risks and threats associated with each system and service;
- Determining the likelihood the risk or threat could occur;
- Identifying and evaluating various methodologies to mitigate the risks or threats;
- Developing the policies and procedures to address the risks or threats;
- Monitoring, and adjusting if necessary, the policies and procedures to achieve the desired results;
- Reviewing policies and procedures at least annually; and
- Training and educating staff.

Operations Impact

Corporate examiners should consider the following when assessing the IST area:

1. Strategic Plan & Goals:
    a. Has management developed a strategic plan for the corporate's IST systems and services?
    b. Has management developed strategic goals, policies, and procedures to implement the strategic plan?
    c. Are those strategic goals, policies, and procedures adequate? They should consider at least, the following items:
        i. Size and complexity of the corporate;
        ii. Types of services offered;
        iii. Volume of IST activity;
        iv. Member demand, usage, and expectations, and
        v. Criticality of systems and services

Critical or non-critical. Management must determine whether IST systems and services are critical or non-critical to the corporate's operations. Management should base this determination on factors including: risk exposure (transaction, security, compliance, reputation, etc.), type of services offered, transaction volume (number and dollar), interconnectivity impact with other systems, member usage, and member expectations and perceptions.

2. Risk Analysis:
    a. Has management performed a risk analysis? The analysis should include at least the following considerations:
        i. Assessment;
        ii. Impact analysis/evaluation;
        iii. Mitigation;
        iv. On-going/periodic monitoring; and
        v. Reporting procedures

3. Policies:
    a. Has management developed appropriate and adequate policies? The policies should address at least the following points:
        i. Security;
        ii. Compliance;
        iii. Business continuity;
        iv. Disaster recovery; and
        v. Vendor management

4. Oversight:
    a. Does management provide adequate oversight? The oversight should include at least the following items:
        i. Adequate staffing;
        ii. Knowledgeable/informed staff; and
        iii. Adequate reporting procedures at various management levels
    b. Has the internal and/or external review program been modified to include reviewing procedures for IST activity?
    c. Does management address issues/concerns effectively, adequately, and timely?
    d. Does management have adequate vendor oversight policies, procedures, and practices?

Examination Objectives

The objectives for reviewing the information system processing are to:

1. Determine if the corporate's policies, procedures, and internal controls are adequate to monitor and control data processing risk.

2. Determine that the corporate complies with the FCU Act, NCUA Rules and Regulations, NCUA issued Directives, the Accounting Manual for Federally Insured Credit Unions, and GAAP, as they directly or indirectly apply to information system processing.

3. Evaluate the adequacy of security policies relative to the risk to the institution.

4. Evaluate vendor management related security controls.

5. Assess the adequacy of the corporate's security controls.

6. Initiate corrective action when the corporate's internal IST controls, policies, procedures, and practices are deficient.

Examination Procedures

See Corporate Examination Procedures - Information Systems Processing (OCCU 303P).

Examination Questionnaire

See Corporate Examination Questionnaire - Information Systems Processing (OCCU 303Q).

References

1. Regulatory Handbook- Thrift Activities Volume I (OTC)

2. NCUA Rules and Regulations (Expanded Authorities Appendices)

3. FFIEC Information Technology Handbooks

4. OCCU Guidance Letters

APPENDIX 303A
IST Glossary of Terms

This glossary of terms is not intended to be a comprehensive list. It focuses primarily on terms that relate to networks, network security, communications, and communication devices used on the Internet. An additional source of definitions can be found at http://whatis.techtarget.com/.

Term — Discussion

Access Control List
An access control list (ACL) is a table that tells a computer operating system which access rights each user has to a particular system object, such as a file directory or individual file. Each object has a security attribute that identifies its access control list. The list has an entry for each system user with access privileges. The most common privileges include the ability to read a file (or all the files in a directory), to write to the file or files, and to execute the file (if it is an executable file, or program). Windows NT, Novell's Netware, Digital's OpenVMS, and UNIX-based systems are among the operating systems that use access control lists. The list is implemented differently by each operating system.

Account Lockout
This feature is available in most current network operating systems. After a specified number of logon attempts, the account is locked out and it usually requires a network administrator to unlock the account.

Administrator Account
This account manages the workstation’s user account, policies and resources. This account cannot be locked out or disabled. The Administrator account also controls files owned by other users.

Alpha Test
The first stage of testing a new software product, carried out by the developer’s staff.

Anonymous FTP
Using the Internet's File Transfer Protocol (FTP), anonymous FTP is a method for giving users access to files so that they don't need to identify themselves to the server. Using an FTP program or the FTP command interface, the user enters "anonymous" as a user ID. Usually, the password is defaulted or furnished by the FTP server. Anonymous FTP is a common way to get access to a server in order to view or download files that are publicly available. If someone tells you to use anonymous FTP and gives you the server name, just remember to use the word "anonymous" for your user ID. Usually, you can enter anything as a password.

API -Application Programming Interface
Software that allows a specific front-end program development platform to communicate with a particular back-end database engine, even when the front end and back end were not built to be compatible.

Applet
An applet is a little application program. Prior to the World Wide Web, the built-in writing and drawing programs that came with Windows were sometimes called "applets." On the Web, using Java, the object-oriented programming language, an applet is a small program that can be sent along with a Web page to a user. Java applets can perform interactive animations, immediate calculations, or other simple tasks without having to send a user request back to the server.

Application
A computer program or set of programs that perform the processing of records for a specific function.

APPENDIX 303A
IST Glossary of Terms

Archie

Archie is a program that allows you to search the files of all the Internet FTP servers that offer anonymous FTP access for a particular search string. Archie is actually an indexing spider that visits each anonymous FTP site, reads the entire directory and file names, and then indexes them in one large index. A user can then query Archie, which checks the query against its index. To use Archie, you can Telnet to a server that you know has Archie on it and then enter Archie search commands. However, it's easier to use a forms interface on the Web called ArchiePlex.

Auditing policies

A critical component of security monitoring controls. Auditing measures the system status against a pre-determined system setting and either will not permit a change or audit and send notifications of the change.

Authentication

The process of proving the claimed identity of an individual user, machine, software component or any other entity.

Bandwidth

The transmission capacity of a computer channel or communications line.

Bastion Host

A computer system that must be highly secured because it is vulnerable to attack, usually because it is exposed to the Internet and is a main point of contact for users of Internal networks. A web page server is an example of a bastion host. It gets its name from the highly fortified projections on the outer walls of medieval castles.

BDC - Back Up Domain Controllers

After a domain has been created, the entire account database is mirrored on each BDC. The PDC (see definition of PDC – primary domain controller) updates a BDC with changes usually at a minimum of every 5 minutes.

Callback security

A feature of remote access servers or software. When a user dials into a remote access facility, the server disconnects the session, and then calls the client back at a preset telephone number or at a number provided during the initial call.

CHAP – Challenge Handshake Authentication Protocol

CHAP (Challenge-Handshake Authentication Protocol) is a more secure procedure for connecting to a system than the Password Authentication Procedure (PAP). Here's how CHAP works:

After the link is made, the server sends a challenge message to the connection requestor. The requestor responds with a value obtained by using a one-way hash function. The server checks the response by comparing it to its own calculation of the expected hash value. If the values match, the authentication is acknowledged; otherwise the connection is usually terminated.

Communications Protocol

A convention—a set of rules and procedures—for completing a communications systems task.

Corporate Security Policy

Defines the assets of a corporation, risks to those assets, owners of these assets and how to protect those assets. It includes creating security awareness among employees and having senior management support. It also defines the framework under which the entire corporation treats and reacts to attacks on its resources.

CRC – Cyclic Redundancy Check

An error-checking procedure for data transmission. The sending device performs a complex calculation, generating a number based upon the data being transmitted, and sends that number to the receiving device. The receiving device performs the same calculation after transmission. If the results match, the transmission succeeds. If the numbers don't match, it means the message was received in an altered state, and the data may be incorrect.

De-militarized Zone

In computer networks, a DMZ (demilitarized zone) is a computer host or small network inserted as a "neutral zone" between a company's private network and the outside public network. It prevents outside users from getting direct access to a server that has company data. (The term comes from the geographic buffer zone that was set up between North Korea and South Korea following the war in the early 1950s.) A DMZ is an optional and more secure approach to a firewall and effectively acts as a proxy server as well.

Denial of service attack

A denial of service attack is aimed at preventing owners of a computer system from using it. It attempts to prevent the use of a system either by using all available processor resources, memory resources, network resources or by shutting down the system. A typical denial of service attack is to send a flood of e-mail messages to a mail server. If the mail server is inside a critical network, the traffic will either close down or severely slow it down.

DES - Data encryption Standard

A standardized encryption method widely used on the Internet.

Digital certificate

A digital certificate is an electronic "credit card" that establishes your credentials when doing business or other transactions on the Web. It is issued by a certification authority (CA). It contains your name, a serial number, expiration dates, a copy of the certificate holder's public key (used for encrypting and decrypting messages and digital signatures), and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real. Digital certificates can be kept in registries so that authenticated users can look up other users' public keys.

Digital Signature

A digital signature (not to be confused with a digital certificate) is an electronic rather than a written signature that can be used by someone to authenticate the identity of the sender of a message or of the signer of a document. It can also be used to ensure that the original content of the message or document that has been conveyed is unchanged. Additional benefits to the use of a digital signature are that it is easily transportable, cannot be easily repudiated, cannot be imitated by someone else, and can be automatically time-stamped. A digital signature can be used with any kind of message, whether it is encrypted or not, simply so that the receiver can be sure of the sender's identity and that the message arrived intact. A digital certificate contains the digital signature of the certificate-issuing authority so that anyone can verify that the certificate is real.

Directory Replication

Any process that utilizes directory replication makes an exact copy of a file contents and places it on another server.

DNS – Domain name system

The DNS is a static, hierarchical name service used with TCP/IP hosts, and is housed on a number of servers on the Internet. Basically, it maintains a database for figuring out and finding (or resolving) host names and IP addresses on the Internet. This allows users to specify remote computers by host names rather than numerical IP addresses. The advantage of the DNS is that you don't have to remember numerical IP addresses for all the Internet sites you want to access.

Domain

A group of computers containing domain controllers that share account information and have one centralized accounts database. The four domain models – single domain, complete trust, master domain, and multiple-master domain-represent various stages of growth and decentralization.

Domain controller

Authenticates users and grants them access to other resources within the network.

Encryption

The process of enciphering or encoding data so that it is inaccessible to unauthorized users.

Ethernet

A standard and probably the most popular connection type for LANs. It was first developed by Xerox, and later refined by Digital, Intel and Xerox (see also "DIX"). In an Ethernet configuration, computers are connected by coaxial or twisted-pair cable where they contend for network access using a Carrier Sense Multiple Access with Collision Detection (CSMA/CD) paradigm.

Event Log

Network operating system services that records system, security, and applications events in the Event Log files.

Event Viewer

A tool used to review logged and audited events. It can be a tool within the operating system or an application designed to do this.

Extranet

The part of a company or organization's internal computer network that is available to outside users, for example, information services for customers.

Finger

Finger is a program that tells you the name associated with an e-mail address. It may also tell you whether they are currently logged on at their system or their most recent logon session and possibly other information, depending on the data that is maintained about users on that computer. Finger originated as part of BSD UNIX. To finger another Internet user, you need to have the finger program on your computer or you can go to a finger gateway on the Web and enter the e-mail address. The server at the other end must be set up to handle finger requests. A ".plan" file can be created for any user that can be fingered. Commonly, colleges, universities, and large corporations set up a finger facility.

Firewall

A combination of devices and software that form a barrier between a secure network and an open environment. Firewalls examine incoming and outgoing communications on a network and determine if the traffic is permissible. Unauthorized communications are not permitted.

FTP - (file transfer protocol)

FTP is a method of transferring files over any network. It is used extensively over the Internet. Typical FTP servers are established for the purpose of giving open access to information. Critical files should never be installed on an FTP server. FTP servers typically should be placed outside a critical network.

Gopher

Gopher is an Internet application protocol in which hierarchically-organized file structures are maintained on servers that themselves are part of an overall information structure. Gopher provided a way to bring text files from all over the world to a viewer on your computer. Popular for several years, especially in universities, Gopher was a step toward the World Wide Web's Hypertext Transfer Protocol (HTTP). With hypertext links, the Hypertext Markup Language (HTML), and the arrival of a graphical browser, Mosaic, the Web quickly transcended Gopher. Many of the original file structures, especially those in universities, still exist and can be accessed through most Web browsers (because they also support the Gopher protocol). Gopher was developed at the University of Minnesota, whose sports teams are called "the Golden Gophers."

Group accounts

Accounts used for grouping together users who perform the same task or require access to the same resources. Group accounts eliminate the administrative headaches that would be created by granting resources to users on a per user basis.

Groups (Global)

Created on domain controllers and used to assign local permissions to domain users. The sole purpose of a global group is to gather users together at the domain level so that they can be placed in appropriate local groups. (see also local groups).

Groups (Local)

Local groups are defined on each machine and may have both user accounts and global groups as members but cannot contain other local groups.

Guest Account

Typically, this account is built into the operating system. It is designed for one time or occasional users. The problem with guest accounts is that they provide no audit trail or user accountability. They should rarely, if ever, be enabled.

HTML - Hyper Text Markup Language

The language in which World Wide Web documents are formatted. It defines fonts, graphics, hypertext links, and other details.

HTTP - Hypertext Transfer Protocol

The protocol most often used to transfer information from World Wide Web servers to browsers, which is why Web addresses begin with http://. Also called Hypertext Transport Protocol.

IMAP – Internet message Access Protocol

A standard protocol for accessing e-mail from your local server. IMAP (the latest version is IMAP4) is a client/server protocol in which e-mail is received and held for you by your Internet server. You (or your e-mail client) can view just the heading and the sender of the letter and then decide whether to download the mail. You can also create and manipulate folders or mailboxes on the server, delete messages, or search for certain parts or an entire note. IMAP requires continual access to the server during the time that you are working with your mail.

Intranet

A private network that uses Internet software (Web browsers, gophers, etc.) and standards (TCP/IP, FTP, HTML, etc.).

IP - Internet Packet

The IP part of TCP/IP; the protocol that is used to route a data packet from its source to its destination over the Internet.

IPX/SPX

(Internet work Packet Exchange/Sequenced Packet Exchange) Protocol used to connect Novell networks.

ISDN - Integrated Service Digital Network

A communications service that encodes voice, data, facsimile, image, and video communications digitally so that they can be transmitted through a single set of standardized interfaces.

Land Attack

A denial of service attack in which the source and destination SYN (see definition of SYN) packets have the same address and the same port. This attack forces the computer to operate more slowly while trying to respond to packets sent to itself.

Latency

In a network, latency, a synonym for delay, is an expression of how much time it takes for a packet of data to get from one designated point to another. In some usages (for example, AT&T), latency is measured by sending a packet that is returned to the sender and the round-trip time is considered the latency.

Logon scripts

Scripts are used to start applications or send environment variables for specific users or computers upon logon.

Nbstat

Tool used to display the contents of a remote computer's Net BIOS name table. The information listed in the Net BIOS name table can be used to determine the Domain name or workgroup the machine is in and the currently connected users. The information may also be used to uncover the Administrator's account due to the fact that account Station IDS are displayed in the name cache.

Net BIOS

Protocol used when Microsoft networking is required in a large multi-segment network. Net BIOS has many similarities to NetBEUI except for the fact that it can be routed with either the TCP/IP or NWLink protocols in a form known as an encapsulated protocol.

NetBEUI - (Net BIOS Extended User Interface)

The built-in protocol of Microsoft networking supports communication in a Microsoft-only environment when the network is small and composed of a single network segment. NetBEUI is a non-routable protocol, meaning that its packets contain no routing information and cannot pass through routers into other network segments.

Netstat

Tool used to display the status of the TCP/IP stack including what ports are open and what connections are active.

Network DDE

Service that provides a network transport as well as secured for DDE (Dynamic Data Exchange) Conversations.

NOS – Network Operating System

Software that controls the execution of network programs and modules.

NTFS - (New Technology File System)

The file system exclusive to Windows NT 4.0 Utilizes Windows NT File and Directory Security features so it is more secure than the File allocation Table File System (FAT) found in Windows 98, 95 and DOS systems.

Nwlink

Microsoft's implementation of the IPX protocol that allows connectivity between the Windows NT and the Novell NetWare Environment.

OFX - Open Financial Exchange

Open Financial Exchange is a unified specification for the electronic exchange of financial data between financial institutions, business and consumers via the Internet. Open Financial

Exchange, which supports transactional Web sites, thin clients and personal financial software, streamlines the process financial institutions need to connect to multiple customer interfaces, processors and systems integrators. By making it more compelling for financial institutions to implement online financial services, Open Financial Exchange will help accelerate the adoption of online financial services by financial institutions and their customers.

OLE – Object Linking and Embedding

A Microsoft Windows capability in which an object from one application can be referenced from within another application.

OSI - Open Systems Interconnection

Standards for the exchange of information among systems that are "open" to one another by virtue of incorporating International Organization for Standardization (ISO) standards. The OSI reference model segments communications functions into seven layers. Each layer relies on the next lower layer to provide more primitive functions and, in turn, provides services to support the next higher layer.

Out of-Band Attacks

Service attacks where data is sent out the normal expected band that has been shown to affect Windows NT. This attack may cause Windows NT to have trouble handling any network operations.

Packet Filtering

The action a device takes to selectively control the flow of data to and from a network. Pack filters allow or block packets, usually while routing them from one network to another (most often from the Internet to an internal network or vice versa). To accomplish packet filtering, you set up a set of rules that specify what types of packets (for example, those to or from a particular IP address or port) are to be allowed and what types are to be blocked. Packet filtering may occur in a router, in a bridge or on an individual host computer.

PAP – Password Authentication Protocol

One of the many authentication methods that can be used when connecting to an ISP. PAP allows you to login automatically, without having to use a terminal window to type in your username and password. One warning about PAP: passwords are sent over the connection in text format, which means there is no protection if someone is "listening-in" on your connection.

PDC - Primary Domain Controller

The central server in the network that maintains the security database for that domain.

Performance Monitor

Tools configured to monitor system performance in Windows NT. It gathers vital information on system statistics and provides the information graphically. It can also be configured to send alerts when a hacker may be attempting to compromise security.

PING - (Packet InterNet Groper)

A standard TCP/IP network utility that sends packets from one machine to another in order to determine if there is a valid network route between them.

Ping-of- Death 2 attack

A variation on the original Ping-of -Death whereby multiple packets of either greater than 64 K in size or multiple 64 K fragmented packets are sent, crashing the receiving system.

Ping-of-Death attack

A security attack involving Ping. Issuing a Ping pack of larger than normal size set at 64 Kbytes causes the Ping-of-Death. This attack effectively takes the system off-line until it is rebooted.

POP3 – Post Office Protocol 3

The most recent version of a standard protocol for receiving e-mail. POP3 is a client/server protocol in which e-mail is received and held for you by your Internet server. Periodically, you (or your client e-mail receiver) check your mail-box on the server and download any mail.

Port

On computer and telecommunication devices, a *port* (noun) is generally a specific place for being physically connected to some other device, usually with a socket and plug of some kind. Typically, a personal computer is provided with one or more serial ports and usually one parallel port. The serial port supports sequential, one bit-at-a-time transmission to peripheral devices such as scanners and the parallel port supports multiple-bit-at-a-time transmission to devices such as printers.

2) In programming, a port (noun) is a "logical connection place" and specifically, using the Internet's protocol, TCP/IP, the way a client program specifies a particular server program on a computer in a network. Higher-level applications that use TCP/IP such as the Web protocol, HTTP, have ports with pre-assigned numbers. These are known as "well-known ports" that have been assigned by the Internet Assigned Numbers Authority (IANA). Other application processes are given port numbers dynamically for each connection. When a service (server program) initially is started, it is said to bind to its designated port number. As any client program wants to use that server, it also must request to bind to the designated port number.

Port numbers are from 0 to 65536. Ports 0 to 1024 are reserved for use by certain privileged services. For the HTTP service, port 80 is defined as a default and it does not have to be specified in the Uniform Resource Locator (URL).

3) In programming, to port (verb) is to move an application program from an operating system environment in which it was developed to another operating system environment so it can be run there. Porting implies some work, but not nearly as much as redeveloping the program in the new environment. Open standard programming interfaces (such as those specified in X/Open's UNIX 95 C language specification and Sun Microsystems's Java programming language) minimize or eliminate the work required to port a program. Also see portability.

PPP - Point-to-Point Protocol

Enables links between two points with no devices in between.

PPPMP - Point-to-Point Protocol Multilink Protocol.

An Internet standard allowing multiple protocols, such as NETBUI and IPX to be encapsulated within IP data grams and transmitted over public backbones such as the Internet.

PPTP - Point-to Point Tunneling Protocol

A Microsoft protocol under which remote users can connect to corporate networks through secure channels creating connections commonly referred to as Virtual Private Networks (VPNS). There are two implementations of PPTP today. One is a North American version featuring 128-bit encryption and the other is an exportable version with 40-bit encryption. (See also Virtual Private Networks).

Protocols

Languages used by computers. In order for two computers to talk to each other, they must use the same protocol.

Proxy server

A server between a client workstation on a network and the Internet. A proxy server is a server that acts as an intermediary between a workstation user and the Internet so that the enterprise can ensure security, administrative control, and caching service. A proxy server is associated with or part of a gateway server that separates the enterprise network from the outside network and a firewall server that protects the enterprise network from outside intrusion.

Public Key cryptography

Public key cryptography consists of a public key and a private key. The public key is given freely to anyone that needs it. The private key is kept secret by the owner of the key and is stored in the user's security file.

Public Key Infrastructure

Public Key Infrastructure (PKI) provides an encryption scheme offering privacy and user authentication. The concept uses a public key accessible by anyone, a private key for decrypting data encoded with your public key, and a pass code to protect your private key. Some experts believe PKI, when implemented properly, is more secure than your own signature.

PVC – Permanent virtual circuit

A software-defined logical connection in a frame relay network. A feature of frame relay, making it a highly flexible network technology is that users (companies or clients of network providers) can define logical connections and required bandwidths between end points and let the frame relay network technology worry about how the physical network is used to achieve the defined connections and manage the traffic.

Query language

A set of commands through which users can update, ask questions, and retrieve data from computer files.

RAID - (Redundant Array of inexpensive disks)

Enables a system to segment data and store pieces of it on several different drives, using a process known as data striping. The principal reason for implementing RAID is for fault tolerance.

RDB – Relational Database

A database in the form of tables which have rows and columns to show the relationships between items, and in which information can be cross-referenced between two or more tables to generate a third table. A query language is used to search for data. If data is changed in one table, it will be changed in all related tables. A database that has only one table is called a flat file database.

Registry

This is the database for windows NT. It contains all the system and program configuration parameters. It also contains the Security Access Manager and configuration data for applications, hardware and device drivers. It also houses data on user-specific profiles, desktop settings, software configurations and network settings.

Remote Access Service

A default service that enables users to connect over a phone line to a network and access resources as if they were at a computer connected directly to the network.

Replication

Creating and maintaining a duplicate copy of a database or file system on a different computer, typically a server. The term usually implies the intelligent copying of parts of the source database which have changed since the last replication with the destination. Replication may be one-way or two-way. Two-way replication is much more complicated because of the possibility that a replicated object may have been updated differently in the two locations in which case some method is needed to reconcile the different versions.

Rlogin

Rlogin is very similar to telnet and is available on many Unix and Non-Unix machines. Rlogin allows you to be on a local machine and to sign on to a remote machine (just like telnet). Rlogin may also require a password to allow system access. However, if it was set up in its default mode, chances are high that a password is not required.

Router

On the Internet, a router is a device or, in some cases, software in a computer, that determines the next network point to which a packet should be forwarded toward its destination. The router is connected to at least two networks and decides which way to send each information packet based on its current understanding of the state of the networks it is connected to.

SAM - Security Access Manager

A data base that maintains all user, group, and workstation accounts in a secure database.

Server Alerts

Used to send notification messages to users or computers. Server alerts are generated by the system, and relate to server and resources use. They warn about security and access problems and server shutdown because of power loss when the UPS service is available.

Share

Created by granting a particular resource a share name. This name is what other users or devices recognize as the entity with which they have permission to access. Shares can be set up on files, folders, directors or server services, such as printing.

Share-level security

Used to give other users access to a local hard drive via the network. The four types of share permissions are No Access, Read, Change, and Full Control.

SLIP - serial line Internet Protocol

An older protocol used to carry TCP/IP over low-speed serial lines.

SMB - Server Message Block

Services that form the backbone of Microsoft networking in the Windows NT environment. All file and printer sharing in Windows NT operate using the SMB services.

SMTP – Simple Mail Transfer Protocol

A TCP/IP protocol used in sending and receiving e-mail. However, since it's limited in its ability to queue messages at the receiving end, it's usually used with one of two other protocols, POP3 or IMAP that let the user save messages in a server mailbox and download them periodically from the server. In other words, users typically use a program that uses SMTP for sending e-mail and either POP3 or IMAP for receiving messages that have been received for them at their local server.

SNMP - Simple Network Management Protocol

An Internet standard for monitoring and configuring network devices. An SNMP network is composed of management systems and agents.

SPAMMING

An inappropriate attempt to use a mailing list, or USENET or other networked communications facility as if it was a broadcast medium (which it is not) by sending the same message to a large number of people who didn’t ask for it.

SSL - Secure Sockets Layer

SSL (Secure Sockets Layer) is a program layer created by Netscape for managing the security of message transmissions in a network. Netscape's idea is that the programming for keeping your messages confidential ought to be contained in a program layer between an application (such as your Web browser or HTTP) and the Internet's TCP/IP layers. The "sockets" part of the term refers to the sockets method of passing data back and forth between a client and a server program in a network or between program layers in the same computer. Netscape's SSL uses the public-and-private key encryption system from RSA, which also includes the use of a digital certificate. This standard was offered free to the Internet community and is now widely used as part of the protocol for transmitting confidential data over the Internet.

SYN

A segment used in the start of a TCP connection to enable both devices to exchange information defining characteristics about the session. It is also used to synchronize the target and destination devices.

SYN flood attack

A SYN is a TCP request that can be sent to a server. When a flood of SYN requests are sent to a single server, the server can only respond with a reset to all further connection requests.

System Alerts

Critical security controls that help perform real-time monitoring of system resources, administrator and user activities. Alerts are configured in the network operating system typically the network administrator.

T1

A telephone line connection for digital transmission that can handle 24 voice or data channels at 64 kilobits per second, over two twisted pair wires. T-1 lines are used for heavy telephone traffic, or for computer networks linked directly to the Internet.

TCP/IP (Transmission Control Protocol/Internet Protocol)

An industry-standard suite of protocols designed for local and wide-area networking. Widely used for Internet communications.

Telnet

The Internet standard protocol to connect to remote terminals. Telnet clients are available for most platforms. When you Telnet to a UNIX site, for example, you can issue commands at the prompt as if you were directly at the machine.

Trojan Horse

In computers, a Trojan horse is a program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can get control and do its chosen form of damage, such as ruining the file allocation table on your hard disk. In one celebrated case, a Trojan horse was a program that was supposed to find and destroy computer viruses. A Trojan horse can be considered a virus if it is widely redistributed. The term comes from Homer's Iliad. In the Trojan War, the Greeks presented the citizens of Troy with a large wooden horse in which they had secretly hidden their warriors. During the night, the warriors emerged from the wooden horse and overran the city.

Trust relationship

A secure communications channel is established between domain controllers. Only servers with proper access rights can send and receive information across this channel. There are two types of trust relationships. The trusting domain which allows another domain to access its resources and the trusted domain-users in the trusted domain can access resources in a trusting domain.

UNIX

A Multitasking Operating System developed in 1969. There are many variants of Unix. Written in the C Programming Language it is very portable - running on a number of different computers. Unix is the main operating system used by Internet host computers.

Untrusted Network

Any network in which secure communications have not been established between domain controllers. The largest untrusted network is the Internet.

UPS Uninterruptible power supply

A power system that provides short term power to critical computers so that in the event of a full power outage, the equipment can continue to operate until it can be safely shut down.

VPN - Virtual Private Network

A combination of software and hardware components that use public networks to create what appears to be a private network. A VPN-based remote access connection typically begins with a data connection to an Internet Service Point of Presence Server. From there, the data flows through a VPN session over the Internet (or other IP network) and ends at the corporate network gateway. All of the data that traverses the Internet is encrypted and authenticated providing the necessary security.

WAIS

Wide-area information servers (WAIS) is an Internet system in which specialized subject databases are created at multiple server locations, kept track of by a directory of servers at one location, and made accessible for searching by users with WAIS client programs. The user of WAIS is provided with or obtains a list of distributed databases. The user enters a search argument for a selected database and the client then accesses all the servers on which the database is distributed. The results provide a description of each text that meets the search requirements. The user can then retrieve the full text.

Whois

An Internet program (related to Finger) that lets you enter an Internet entity (such as domains, networks, and hosts) and display information such as a person's company name, address, phone number and email address.

Chapter 304

ITEM PROCESSING SERVICE CENTERS

Introduction

Item processing is the conversion of source documents, checks, and other transaction tickets to machine readable form, then processing and distributing this information in a manner that results in the ultimate settlement (payment or collection) through the Federal Reserve Bank (FRB) or another correspondent financial institution. Item processing services are performed by larger natural-person credit unions, corporate credit unions (corporates), credit union service organizations (CUSOs), leagues, banks, and national or regional check processing service centers.

Item processing services are and will continue to change. With the advent of Check 21, the increase in electronic funds transfer, the use of ACH and internet bill payment, the utilization of paper checks is declining. The FRB continues to consolidate its check processing units at a number of its faciltities throughout the country. This restructuring will create additional opportunities as well as increased competitive pressures for corporates.

Share Draft Inclearing

Share draft inclearing is a common item processing service. This refers to the corporate's processing of member credit union share drafts. The following steps occur in this process:

1. A credit union member pays a vendor with a share draft, which the vendor deposits into its bank account.

2. The bank processes this deposit internally by encoding and sending the share draft to the FRB for credit.

3. The FRB processes the share draft, credits the local bank's account at the FRB and charges the credit union's payable account through the corporate's account at the FRB.

4. The FRB sends the corporate (by courier) the cleared member share draft.

5. The corporate sorts and images the member share draft and posts the inclearing transaction from the FRB to the member share draft account.

6. Share draft exception reports run the next morning by the member credit union will identify any account with insufficient funds, closed or non-existent accounts, or other criteria that prevents the draft from being paid. Returns are initiated by the member credit union to the corporate.

7. The corporate physically pulls the item and sends it back to the FRB for return to the local bank and gives the member credit union immediate credit.

Deposit Transit

Deposit transit (collection) is another common item processing service performed by corporates. This occurs when a corporate receives and processes checks which have been deposited at a member credit union for credit to the individual member accounts. The basic process follows:

1. The member sends the day's check deposits (by courier) to the corporate.

2. The corporate processes, images, sorts, and sends the checks to the FRB for credit (the encoding may be performed by the credit union or corporate, depending on the arrangement).

3. The FRB receives the check deposits (in the form of a cash letter) and then processes the checks.

4. The account at the FRB payable through the corporate is credited. At the same time the accounts for the banks paying the deposited checks are charged for the payments and the checks are sent to those banks or their designated processor.

Direct Presentment Arrangements

Direct presentment arrangements occur when two or more financial institutions, in a defined geographical area, agree to directly present their checks (deposits and payments in the form of cash letters) to each other, bypassing the FRB. These arrangements, in some cases, may involve formation of a local clearing association, with its own procedures and restrictions on joining the association. Direct presentment arrangements can exist for both deposits and share drafts.

Share Draft Clearing via Direct Presentment includes the following steps:

1. A vendor deposits the share draft at its financial institution.

2. The financial institution processes and sorts the checks which are encoded with the corporate's routing and transit number.

3. The checks and a cash letter are sent directly to the corporate for settlement the same day.

4. The corporate proofs the checks, which have been directly presented, to confirm the payment amount on the cash letter and posts the payment amounts to the member share draft clearing accounts.

5. The corporate then pays the local bank (by Fedline wire) for the member share draft deposits made at the bank.

Deposit Settlement via Direct Presentment includes the following steps:

1. The member credit union or participating bank sends the checks deposited that day to the corporate.

2. The corporate sorts the checks. Each participating local bank is sent a cash letter and a bundle of checks issued by that bank with a demand for payment.

3. The bank processes the checks and wires an amount to the corporate to settle payment for its cleared checks.

Item Processing Center Facilities

The most common equipment and related components of the item processing operation are:

1. encoding stations;
2. reader/sorter(s) (includes imaging process);
3. power encoders**;**
4. computer terminals for both the item processor controller and member credit union data systems;

5. reject/re-entry stations;
6. correspondence desks used for resolving and researching differences with members, other financial institutions, and the FRB;
7. check storage areas both on-site and off-site; and
8. microfilming equipment.

Facilities should be organized in a manner that results in an efficient, one-way workflow. The space allocated to item processing operations and related functions must be adequate to assure proper physical segregation of equipment and personnel. The following physical security controls are common:

1. controlled access, via card key or combination locks;
2. fire suppression systems;
3. water detection equipment below the floors;
4. hand-held fire extinguisher(s);
5. switches to activate an alarm when an electrical circuit is broken; and
6. sound and/or motion detection equipment.

In addition to physical controls over the item processing equipment, all negotiable instruments (checks, cash letters, deposits in transit, etc.) should be in a secure area from their initial receipt throughout processing, imaging or filming, storage and destruction.

Document Management and Data Backup

Properly stored and maintained microfilm imaging is essential for all item processing operations. Controls must be in place to safeguard the microfilm imaging stored on-site, and for maintaining at least one full copy off-site. Procedures must be in place to ensure all images are legible prior to placing it in storage. Processed data must be backed up daily. Adequate generations of backed-up data must be maintained both on- and off-site.

Written contracts must be in place documenting agreements for the satisfactory destruction of physical checks, cash letters and reconciliation support. Items should be shred on-site while witnessed by a staff member or transported in secured containers to a vendor location for shredding. Management must provide a sufficient record of the process documenting that the items are adequately destroyed.

Contingency Planning

Management must ensure that plans are in place to resume operations in a timely manner in the event of damage to the facilities and/or equipment. The item processing operation should be included in the corporate-wide contingency plan.

Management must:

1. establish legal agreements for the use of alternate sites and equipment;
2. develop procedures for all item processing operations under full disaster recovery situations; and
3. test fully item processing operations with alternate site equipment. The test must be realistic, comprehensive, and well- documented. Item processing functions must be fully restorable within hours of the time item processing operations are impaired.

Item processing contingency testing should employ sufficient volumes to ensure the processing function could be maintained until standard operations could be fully restored. If there is limited equipment at the back-up site, consideration should be given to temporarily obtaining available resources so comparable volumes can be tested, ensuring the adequacy of the backup function.

Transaction Volume and Trends

Significant investments in hardware, software, and human resources are needed to support item processing operations. High volume operations may require more than one reader/sorter. Backup equipment or backup capabilities are needed at alternate sites, or should be contracted with third parties.

Potential Losses

Human error, fraud, failure to remain competitive, operational disruption, or catastrophic damage to the facility and/or items in transit can cause losses in an item processing operation.

The examiner should review lawsuits, pending litigation, and write-offs. Excessive legal problems and losses stemming from the operation could indicate deficiencies in management, internal controls, and/or contractual agreements.

Policies and Procedures

Comprehensive policies and procedures are needed to manage the risks represented by an item processing operation. The board-level policy or board-directed procedures should address the following, at a minimum:

1. specific services offered;
2. fee structure;
3. periodic cost analysis;
4. market factors, including market penetration studies, assessment of direct competition, and changes in technology (image processing, branch capture, proof of deposit, etc.); and
5. charge-off policies.

The examiner should review workflow procedures which address operational functions in detail. These include but are not limited to:

1. departmental internal control structure;
2. operational deadlines and computer run schedules;
3. accounting procedures and requirements;
4. reject/re-entry and return procedures;
5. timely research and clearing of suspense items;
6. disaster recovery procedures;
7. personnel management, including cross-training and back-up schedules;
8. records maintenance and destruction procedures;
9. security measures; and
10. equipment care and maintenance.

Management must routinely review and update procedures, as well as staff's compliance with policies and procedures.

On an ongoing basis, management must monitor item processing operations, accounting reconciliations, clearing of adjustments, and compliance with deadlines. The board of directors should review monthly financial and operational reports regarding the item processing operations. Plans for resolving accounting and adjustment backlogs or problems in operations must be developed and implemented on a timely basis.

Management should develop flowcharts and/or narratives discussing the flow of items (deposits or payments) through the system. Tracing the flow of items through the system should document that:

1. timely and accurate settlement occurs through the FRB or another correspondent bank; and
2. the transactions post accurately to individual members' share accounts.

Contracts with Third Parties

The examiner should review all contracts for item processing services to ensure the following matters are addressed:

1. Settlement line of credit agreements between corporates and credit unions - These are needed to ensure the coverage of check clearing settlements if a member credit union's account balance is insufficient to cover clearings on a given day.

2. Disaster recovery agreements for alternate site and processing equipment - This is essential to ensure continuation of operations in the event of disaster.

3. Maintenance agreements - These are necessary to ensure appropriate software and hardware support and prompt maintenance.

4. Agreements with the FRB and other exchange networks.

5. Agreements with any other hardware and communication vendors for funds settlement and electronic transmission activity.

6. Contract with destruction company or certification of destruction.

Management and Staff Experience

The manager of the item processing department should exhibit a thorough knowledge of each functional area of the operation, as well as possessing management experience. Without a thorough understanding of each function, the manager cannot ensure the overall operation remains as efficient as possible. The manager should also exhibit awareness of new technology and how it might be used to increase the efficiency and/or profitability of the operation.

Cross training is critical in small and medium operations. Even in larger operations, management must have appropriate cross training and back-up plans in place to cover unexpected absences and/or staff turnover.

Staffing levels must be adequate to maintain sufficient internal controls and separation of duties. Computer access controls and security measures must be in place.

Imaging systems can change or eliminate traditional controls, inherent in a paper based system. Internal audit procedures may have to be redesigned. The internal auditor should be involved from the planning stages forward.

Profitability Management

The costs of starting and maintaining an item processing operation are significant. A business plan must be established to identify the services to be provided and the resources needed to operate this area. Departmental cost and revenue projections as well as the impact item processing will have on the corporate's financial performance must be properly documented. The business plan should include:

1. A description of the corporate's operations, internal controls, management, staffing, training, hardware, software, disaster recovery, accounting support, and volume projections.

2. Long- and short-term financial and operational goals.

3. Marketing studies and plans, including analysis of competitors' prices and services, and determination that existing demand and volume are sufficient to support the operation as an ongoing concern.

4. A detailed budget identifying the total expected cost and revenue of the item processing operations under varying volume scenarios. It is recommended that examiners verify projected volume data for reasonableness regarding any corporate considering entering this business on its own or through the purchase of an existing processor.

In support of the business plan, a department profitability analysis should be completed at least annually. Management should ensure all costs of operating the department (e.g. facilities, human resources, internal and external audit, contingency planning, write-offs) are appropriately allocated to the operation. In that way**,** the true cost and profitability of the operation are determined and communicated to management and other users of the analysis. When analyzing profitability, it is important to ensure stable item processing revenues are not based on a combination of increasing clients and declining volume. The trend of declining volume can reasonably be expected to continue while the increase in clients can not. If volumes are declining either on an absolute or per member (credit union) basis, a determination should be made that management has established a stop-loss threshold at which service will be phased-out and appropriately curtailed.

Effective management of an item processing operation includes continually reviewing the operation for areas where efficiency can be increased, and/or operating costs reduced, while maintaining reasonable internal controls and segregation of duties throughout the operation.

Document Imaging

Optical imaging systems provide a method of capturing, storing, displaying, printing, and transmitting data. Such systems offer the opportunity to streamline the item processing department workflow, reduce storage and retrieval costs, and improve customer service through automation. The following must be considered when installing document imaging in an item processing operation:

1. Planning - Poor planning can result in excessive installation costs, loss or destruction of original documents, and failure to achieve expected benefits.

   Issues which should be considered in the planning stages include:

   a. conversion of existing paper storage files;
   b. integrating imaging into the organizational workflow; and
   c. backup and recovery procedures.

2. Scanning Devices - Good quality scanning equipment is critical as these devices are the entry point for all transactions. Workflow can be affected if scanning equipment cannot handle the volume or breaks down. Poor controls over the scanning process can result in poor quality images, improper indexing, or incomplete or forged documents being entered into the system.

3. Indexing - Proper indexing of documents is critical to future retrieval and limiting access to files. The integrity of the indexing must be carefully maintained in order to ensure and control access, as well as protect documents from unauthorized modification. The indexing method also can affect the security administrator's ability to restrict access based on the user's needs.

4. Software Security - System security controls over imaged documents are critical to protect the corporate and its members from unauthorized access and/or modifications to documents. Software security and security administrator functions are essential to prevent unauthorized alterations to stored documents.

5. Contingency Planning – A multitude of documents may be stored on a single optical disk; therefore, the loss of storage files or media can severely impact business if electronic back-up or paper files are not maintained. The overall contingency plan should be modified to address the use of imaging in the item processing operation.

6. Training - Failure to properly train personnel responsible for operating scanning equipment can result in poor quality document images and indices as well as the premature destruction of original documents.

7. Legal Issues - Corporates installing imaging systems should carefully evaluate the legal implications of converting original documents to image, and the subsequent destruction of the original documents. Existing contracts should be reviewed to determine procedural changes are consistent with contract language and requirements.

Branch Capture

Branch capture is a sophisticated method of processing checks that a corporate's member credit union takes in from its membership. Item information is captured at the credit union location by a scanning device. An image of the check or item is then transmitted to the corporate for processing. The original checks can be truncated at the member credit union location and transferring of the items among locations is no longer necessary. The corporate can print the images or transfer them electronically depending on the agreements in place. National networks are being developed to exchange large volumes of images among financial institutions. Financial institutions are also collaborating to directly exchange images.

Branch capture technology also allows corporates to serve its members with proof of deposit services. The credit union can scan its deposits and transmit the information electronically. Once the transfer is balanced and agreed upon the credit union receives settlement of the funds.

The corporate's item processing remains basically the same regarding branch capture. The primary benefit is that items processed through branch capture are transferred electronically, reducing the paper being processed through the reader/sorter. The software and hardware (scanners and data storage) is expensive, which emphasizes the importance of the corporate having a realistic business plan to address costs, pricing and volumes.

It is important that the process and controls involved with the electronic transfer and storage of images is reviewed during the information systems review. Protection of member data is essential for corporate credit unions and the credit union network.

Problem Areas

Common problems found in item processing operations include the following:

1. high staff turnover;
2. inadequately trained personnel;
3. inadequate staffing levels for proper internal control, accounting, and adjustment clearing;
4. changes in settlement patterns or procedures;
5. inadequate communication, hardware, and/or software may result in incorrect postings and reconciliations;
6. rapidly growing volume, added to existing inadequate staffing and inappropriate accounting systems;
7. weak internal controls and accounting procedures; and
8. backlog of reconciling items.

Corporates exhibiting difficulties in new or established item processing operations may benefit from a third party review. A full third party review involves an evaluation of the accounting system controls and day-to-day operations of the department. Large public accounting firms usually have the expertise to review both functions of the department. Weaknesses in operations, management, and accounting identified during a review should result in the development of plans for prompt corrective action.

Regulatory Considerations

The following are two laws significantly impacting item processing and the security of personal information.

Check Clearing for the 21st Century Act

This law is commonly referred to as Check 21. Check 21 went into effect on October 28, 2004. The purpose of this law is to:

- Facilitate check truncation by creation of a new negotiable instrument known as a "substitute check;"
- Foster innovation in the check collection system without mandating receipt of checks in electronic form; and
- Improve the overall efficiency of the nation's payment systems.

The act does not mandate image exchange, provide any legal coverage for image exchange, or determine what constitutes legal presentment.

Gramm-Leach-Bliley Act (GLBA)

This act is also know as the Financial Services Modernization Act of 1999. The GLBA's privacy protections only regulate financial institutions. Financial institutions, whether they wish to disclose personal information or not, must:

- Develop precautions to ensure the security and confidentiality of customer records and information;
- Protect against any anticipated threats or hazards to the security or integrity of such records; and
- Protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.

Examination Objectives

The objectives for reviewing item processing service centers are to:

1. Determine if the corporate's policies, procedures, and internal controls are adequate to monitor and control the risk in its item processing operations.

2. Assess management's guidelines for evaluating and monitoring item processing operations.

3. Determine that corporate management and officials are adhering to established guidelines.

4. Initiate corrective action when the corporate's item processing policies, procedures, practices, and controls are deficient.

Examination Procedures

See Corporate Examination Procedures - Item Processing Service Center (OCCU 304P).

Examination Questionnaire

See Corporate Examination Questionnaire - Item Processing Service Center (OCCU 304Q).

References

1. FFIEC Information Systems Examination Handbook, 1996 Edition
2. NCUA Examiners' Guide, Chapter 24, Item Processing
3. FFIEC Information Technology Examination Handbook: Operations, June 2004

Appendices

304A Common Item Processing Terms
304B Item Processing Schematics

Appendix 304A

C0MMON ITEM PROCESSING TERMS

Adjustment - An entry requested by the corporate, member credit union, other financial institution, or Federal Reserve Bank because another institution has lost an item or cash letter, encoded an item incorrectly, etc.

Bank of First Deposit – The credit union where a member deposits a share draft. Also referred to as the BOFD**.**

Batch Processing - A group of transactions**,** deposits, or check clearings assembled for proving or processing purposes. A batch may consist of 100-300 items. Each batch is accompanied by a batch control ticket which records the batch number, control totals, and routing information.

Cash Letter – Bundles of items deposited or received together based on work type. They are accompanied by a cash letter form summarizing the encloed bundle amounts and the total.

Clear on Tickets - An action initiated by a clearing house bank to debit the corporate for an adjustment.

Fine Sort - A term used to describe sorting transaction media into numerical or alphabetical order.

ICR or Intelligent Character Recognition – This usually refers to the machine reading of handwriting.

Imaging – A term referring to the process of capturing a digital image of share drafts.

Incoming Return Items - Items being returned to the bank of first deposit (also referred to as the BOFD).

Inclearing - A process whereby items are captured, imaged, sorted, and then presented to credit unions for posting to member accounts. Inclearing items include but are not limited to the following:

1. **Convenience Draft** - A draft against a credit card account.
2. **Corporate Draft -** A draft written by a credit union against its own account.
3. **Pre-authorized Draft** - An item initiated by a third party, with authorization by the account holder, to debit the share draft account for payment. Examples of pre-authorized drafts include health club dues, electric bills, and insurance premiums.
4. **Share Draft** - A written draft on a deposit account by a credit union member.

5. **Sight Draft** - An item initiated by a financial institution with an ATM, to debit a credit union for an error that occurred at that ATM, or a return item.

Infirmity - Any known act, or omission, that would invalidate an instrument (share draft). Common examples of infirmities that would cause a financial institution to refuse payment are missing endorsements, missing signatures, conflicting amounts in written and numerical figures, alterations, or forgeries.

IRD or Image Replacement Document – A reproduction of a share draft or the image of a digital share draft.

Item - Any media, excluding coin or currency, handled daily by a financial institution, which will be posted in total or in detail, as a debit or a credit, to an institution’s account. Items are generally referred to by type, such as “cash items,” “transit items,” “on-us items,” clearing items,” “general ledger items,” etc.

MICR - Magnetic Ink Character Recognition. Process used for encoding checks and/or other types of items to be processed. The MICR-line, which contains check routing account number and dollar amount information, is read to capture (read) the item and then sort it.

Mis-sent Item - An item which has been sent in error to another financial institution.

Mis-sort - An item sorted into the wrong account. A mis-sent item leaves the financial institution, while a mis-sorted item remains in the financial institution’s possession, but causes a control problem.

Proof Machine - A machine with multiple pockets designed to balance and encode debit and credit transactions, accumulated pocket and grand totals, and sort the source documents according to type.

Reader/Sorter - A high speed document handler that reads MICR encoded information on documents for transmission to a computer and sorts the MICR documents on digits selected either at the unit console (off-line) or by the computer program (on-line).

Raised Check - A check on which the dollar amount has been illegally increased.

Reject - An item rejected from the reader sorter which has to be processed manually. Reasons for rejection include incomplete or unreadable MICR lines, or invalid check digits/account types.

Return Item - An item the member credit union returns rather than posting to the member’s account. Examples of return items include insufficient funds, stop payments, account closed, unauthorized drawer signature, and uncollected funds. Items must be returned within 24 hours of presentment.

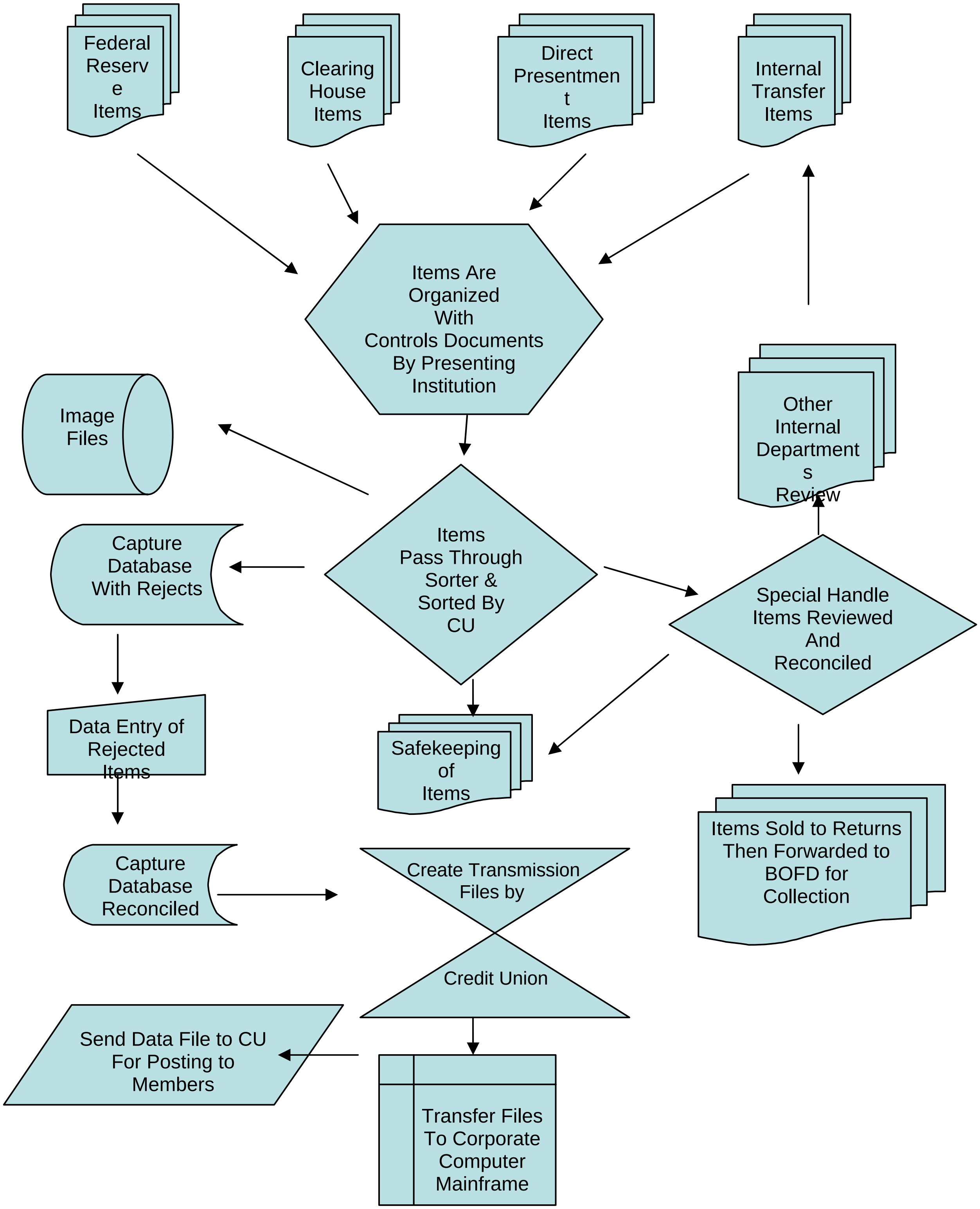
Routing and Transit Number - The numbers printed on checks to identify the specific institution on which a check is drawn and to which the check must be sent for payment by the Federal Reserve.

Transit Item - A cash item drawn on a financial institution outside the immediate exchange area. Transit items are processed and sent to the Federal Reserve Bank(s), correspondent financial institutions, etc., for collection and remittance to the financial institution that originally received the items.

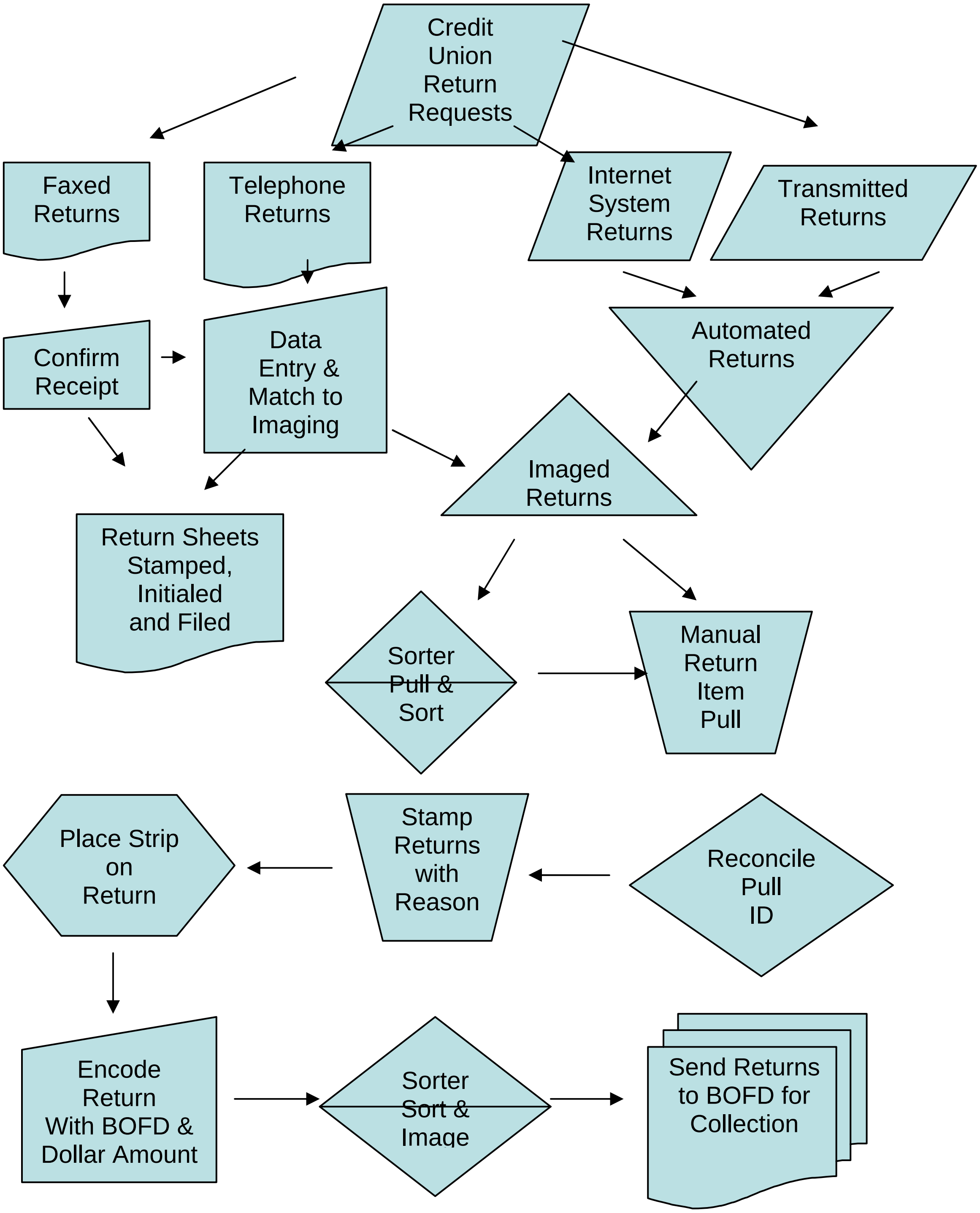
Transit Letter - A deposit form or remittance instruction slip that described and gives totals of items to be collected and paid, enclosed with the checks and other cash items. The term “cash letter” refers to transit items sent to a financial institution where the remitting institution maintains an account. A “remittance letter” is sent when payment must be made (usually by draft) for the items sent.

Truncation - The process of distributing the original copies of cleared share drafts. In truncated processing, drafts are stored for a prescribed number of days (usually 60-90), then confidentially shredded. In non-truncated processing, items are returned to the member credit union and distributed to the members in monthly account statements.

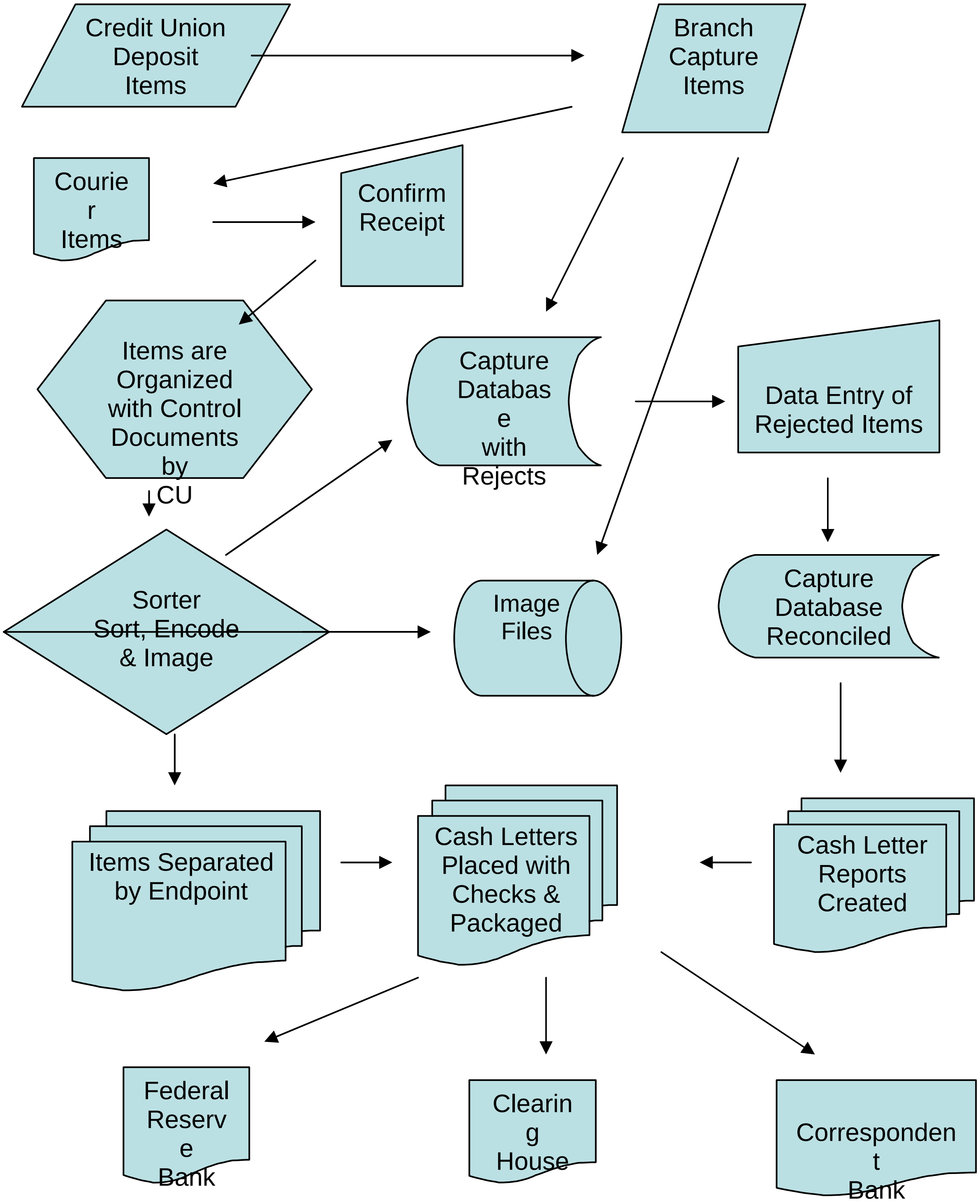
Inclearing Processing


Federal Reserv e Items
Clearing House Items
Direct Presentmen t Items
Internal Transfer Items
Items Are Organized With Controls Documents By Presenting Institution
Image Files
Other Internal Department s Review
Capture Database With Rejects
Items Pass Through Sorter & Sorted By CU
Special Handle Items Reviewed And Reconciled
Data Entry of Rejected Items
Safekeeping of Items
Capture Database Reconciled
Create Transmission Files by
Credit Union
Items Sold to Returns Then Forwarded to BOFD for Collection
Send Data File to CU For Posting to Members
Transfer Files To Corporate Computer Mainframe

Return Item Processing



Deposit Processing


Credit Union Deposit Items
Branch Capture Items
Courie r Items
Confirm Receipt
Items are Organized with Control Documents by CU
Capture Databas e with Rejects
Data Entry of Rejected Items
Sorter Sort, Encode & Image
Image Files
Capture Database Reconciled
Items Separated by Endpoint
Cash Letters Placed with Checks & Packaged
Cash Letter Reports Created
Federal Reserv e Bank
Clearin g House
Correspondent t Bank

Chapter 401

CORPORATE RISK INFORMATION SYSTEM (CRIS)

Introduction

Corporate credit unions (corporates) are unique financial institutions. They are the only institutions, other than Federal Reserve and Federal Home Loan Banks, that exist primarily to provide financial, liquidity, and correspondent services to other financial institutions (e.g., credit unions).

The system used to detect, measure, and monitor these risks must be unique to the environment in which it will be used. Whereas the financial stability of corporates is crucial to their credit union members' success in providing services to their members, a regulatory risk rating system needs to be highly effective in identifying and measuring specific areas of risk during the supervisory process. By accurately detecting and communicating risk areas, NCUA can achieve the most effective supervisory efforts possible, and help avoid a major financial and operational crisis in the corporate credit union system (System).

NCUA's responsibilities to effectively detect, communicate, and control risk within the System, necessitates a highly specialized and effective risk rating system.

NCUA considers management's role in corporates to be the major catalyst in the financial and operational success of the institutions. In order to benefit NCUA, a corporate risk rating system must effectively evaluate, measure, and report the qualitative strengths and weaknesses of management personnel, practices, and policies. This system operates independent of the quantitative risk measures such as empirical levels of capital, earnings, and market risks.

CRIS separates the assessment and communication of quantitative financial risks from qualitative operational and managerial risks and assigns individual Financial Risk and Risk Management Composite and Component Ratings, respectively.

The Financial Risk Composite Rating is:

> An assessment of measurable risk exposure to the corporate's capital, relative to levels of exposure to credit, interest rate, and liquidity risk as of the date of the examination.

The Risk Management Composite Rating is:

> A qualitative risk assessment derived from the examiner's evaluation of management's policies, practices, and expertise in identifying, measuring, monitoring, reporting, and controlling risk.

Used in conjunction, the components allow NCUA to more effectively focus resources in specific areas of risk identified during the supervisory process, and develop and implement appropriate supervision strategies.

The CRIS rating system's examination and supervision objectives are:

1. To detect, evaluate, and measure financial and operational risks;
2. To determine the effect that these risks may have upon the financial (capital) strength of the institutions;
3. To assess the quality of management, policies, and procedures;
4. To assess and control risk to the National Credit Union Share Insurance Fund (NCUSIF); and
5. To provide a rating system, internal to NCUA, that will be used to allocate agency resources for ongoing examination and supervision needs of corporates.

CRIS System

CRIS provides individual composite ratings for both Financial Risk and Risk Management, based upon certain components as follows:

1. The Financial Risk Composite rating is derived by the measurement and interrelationship of five quantitative components: Empirical Capital Level; Earnings; Interest Rate

Risk Exposure; Liquidity Risk Exposure; and Credit Risk Exposure; and

2. The Risk Management Composite rating is similarly derived through the evaluation of seven components stressing the qualitative nature of risk management. These are: Capital Accumulation Planning; Profit Planning and Control; Interest Rate Risk Management; Liquidity Risk Management; Credit Risk Management; Operations Risks; and Board Oversight, Audit & Compliance.

Disclosure of CRIS to Corporates

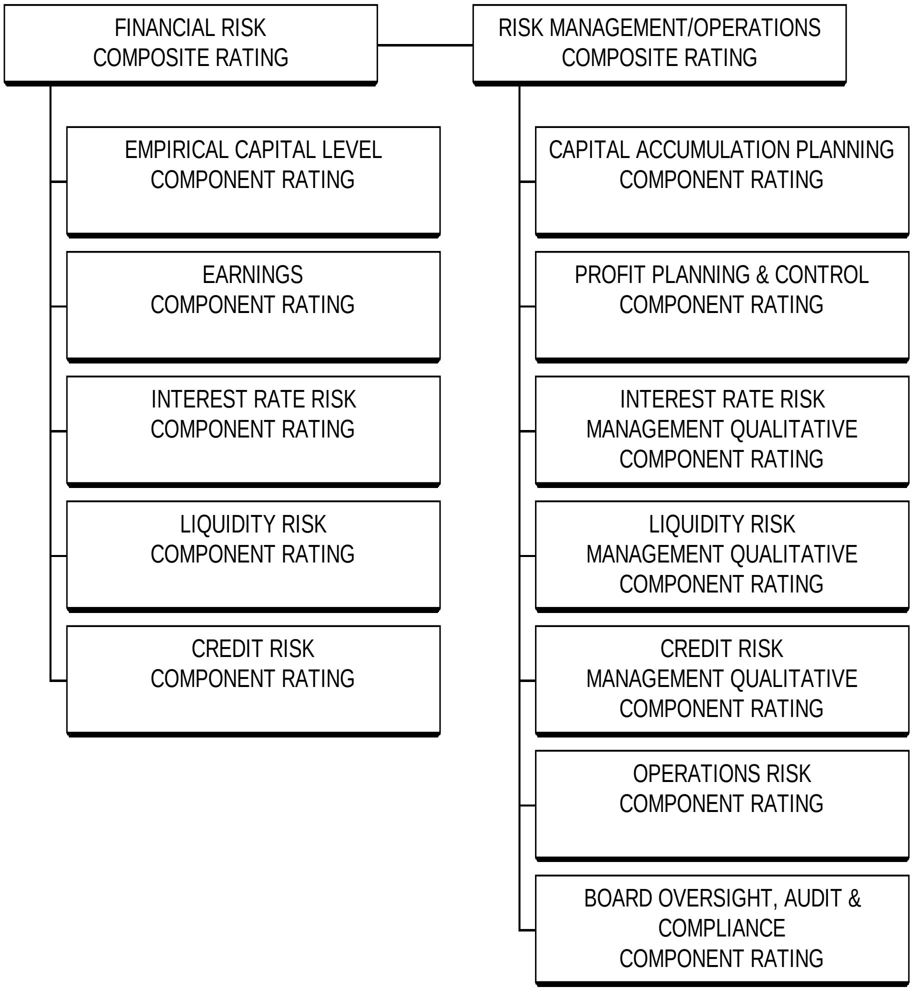
The major emphasis of the examination report will focus on the individual areas of concern identified during the examination and implementing corrective action. However, both the Financial Risk and Risk Management composite and component ratings will be disclosed in the Executive Summary section of the examination report. To eliminate the problem of officials focusing on the ratings as opposed to the issues, the ratings will not be disclosed until after the issues are discussed with a corporate's board during the joint conference.

Coordinating the disclosure of CRIS with State Supervisory Authorities (SSA)

Each SSA has specific procedures for the disclosure of their risk rating systems to state chartered corporates. Examiners should coordinate their efforts with the SSA to ensure that the intent of the agreements reached in the Document of Cooperation and individual agreements with SSAs, as well as the conditions in Chapter 104 of this guide, are met.

The diagram on the next page provides a practical depiction of the CRIS rating system.

CORPORATE RISK INFORMATION SYSTEM (CRIS)


FINANCIAL RISK COMPOSITE RATING
RISK MANAGEMENT/OPERATIONS COMPOSITE RATING
EMPIRICAL CAPITAL LEVEL COMPONENT RATING
EARNINGS COMPONENT RATING
INTEREST RATE RISK COMPONENT RATING
LIQUIDITY RISK COMPONENT RATING
CREDIT RISK COMPONENT RATING
CAPITAL ACCUMULATION PLANNING COMPONENT RATING
PROFIT PLANNING & CONTROL COMPONENT RATING
INTEREST RATE RISK MANAGEMENT QUALITATIVE COMPONENT RATING
LIQUIDITY RISK MANAGEMENT QUALITATIVE COMPONENT RATING
CREDIT RISK MANAGEMENT QUALITATIVE COMPONENT RATING
OPERATIONS RISK COMPONENT RATING
BOARD OVERSIGHT, AUDIT & COMPLIANCE COMPONENT RATING

Interrelationship of CRIS Composites, Components and Evaluation Factors

Under CRIS the corporate will be assigned a Financial Risk and a Risk Management composite rating. The composite ratings are derived through the interrelationship between underlying component ratings. The component ratings are derived through the examination of relevant Evaluation Factors. Examiners will rate the components and composites 1 through 5; 1 being the best and 5 the worst. The risk rankings assigned to the Evaluation Factors will be used to determine the overall component ratings to which they relate. Definitions of component and composite ratings are defined in detail in

Appendix 401A, CRIS Composite and Component Rating Definitions and Evaluation Factors. Assignment of separate Financial Risk and Risk Management Composite Ratings provides a more effective manner of identifying immediate and potential risks to a corporate's financial strength. By providing separate ratings for quantitative (financial risk) and qualitative (risk management abilities) factors, an accurate and effective risk assessment of the corporate can be made.

Evaluation Factors

Evaluation Factors are reviewed as part of the overall examination process by the examination team. Each Evaluation Factor must be assessed by the examiner as it applies to both the corporate's scope of business and any Part 704 Expanded Authorities (if applicable). Evaluation Factors are assigned specific risk rankings based upon the examiner's review and professional judgment. Generally, the risk ranking assigned to each Evaluation Factor should be independent of others. If applicable, certain Evaluation Factors may be given more weight in determining the overall composite. Examiners should use professional judgment when determining whether to place more emphasis on one Evaluation Factor over another when deriving an overall component rating. Each Evaluation Factor is assigned a risk ranking as noted in the tables below:

Financial Risk Component	
Risk Ranking	**Degree of Risk to Capital and/or Earnings**
1	Low Risk
2	Moderate (managed) Risk
3	High Risk
4	Excessive Risk
5	Critical Risk

Risk Management Component	
Risk Ranking	**Quality of Policy or Risk Management Process**
1	Exceptional
2	Acceptable
3	Minimally Acceptable
4	Inadequate
5	Seriously Deficient

The risk rankings assigned to the Evaluation Factors must be derived based on professional judgment of the operating principles and standards in this Corporate Examiner's Guide, the Guidelines for Submission of Requests for Expanded Authority, and other industry accepted standards. The Financial Risk and Risk Management components will be derived as a result of the interrelation of the risk rankings assigned to the individual Evaluation Factors*.*

Composite and Component Ratings

Financial Risk Composite Rating

The Financial Risk Composite Rating is derived, by not only assessing the corporate's empirical level of capital and earnings, but also determining credit, interest rate, and liquidity risk exposures, and the effects these risks could have on the earnings and capital levels. Individual component ratings are assigned to these areas when developing the overall composite rating.

The examiner must keep in mind that the Financial Risk Composite Rating is a quantitative assessment of relative capital strength in relation to earnings performance and financial risks. The Financial Risk Composite Rating is not an arithmetic average of the individual components. The component ratings should be evaluated independently using the guidelines in Appendix 401A and the examiner's judgment to derive and assign the overall Financial Risk Composite Rating. The component ratings are similarly derived through an assessment of the individual Evaluation Factors reviewed as part of the examination scope. Guidelines for examiner assessment of the individual Financial Risk components are provided in specific sections of this chapter, and throughout the Corporate Examiner's Guide. A list of Evaluation Factors is listed in Appendix 401A, along with definitions of the Financial Risk Component and Composite Ratings.

Risk Management Composite Rating

The ability of management to develop appropriate business plans, operational policies and procedures, and risk management policies and practices is crucial to ensure the ongoing financial soundness of each corporate. CRIS acknowledges the importance of management's capabilities by providing a separate and distinct Composite Rating in assessing the abilities and effectiveness of corporate management. The Risk Management Composite Rating should reflect the examiner's assessment of the qualitative factors attributable to the management of financial risk and those inherent within corporate operations (i.e., processes and results that cannot be measured on a numerical basis). The Risk Management Composite Rating will be derived through the assessment of the seven individual Risk Management Component Ratings, as follows:

1. Capital accumulation planning;
2. Profit planning and control;
3. Interest rate risk management;
4. Liquidity risk management;
5. Credit risk management;
6. Operations; and
7. Board oversight, audit & compliance.

The Risk Management Composite Rating is determined as a result of the examiner's review of the corporate's operational processes, policy making and planning capabilities, and risk management and reporting process. The Risk Management Composite Rating is not measured on financial results. This Composite Rating will be assigned as a result of the examiner's review of each component's Evaluation Factors as they relate to the corporate's scope of operation and Expanded Authorities (if applicable).

Assignment of Composite Ratings

The examiner will follow the composite rating definitions outlined in Appendix 401A to assign both the Financial Risk and Risk Management Composite Ratings. OCCU Form 102I will be used to facilitate this process. On OCCU 102I, the examiner in charge (EIC) will assign ratings using team member recommendations; however, the EIC makes the final CRIS rating decisions.

Examiners have the latitude to increase or decrease any component or composite rating based on individual circumstances and/or professional judgment; however, rationale supporting increases and/or decreases should be documented in the confidential section of the examination report. OCCU 102I will be included with the field and office copies of the examination report. The work papers will provide support for the component and composite ratings by listing the risk rankings assigned to the individual Evaluation Factors.

Empirical Capital Level & Capital Accumulation

Since the revision of Part 704 in 1998, corporates have increased retained earnings, some more successfully than others. When reviewing capital, the examiner should specifically address retained earnings trends and ratios in relation to financial and operational risks.

Meeting minimum capital requirements is a key factor in determining capital adequacy. More importantly, the examiner must consider whether the corporate's operations and risk position requires capital above the minimum regulatory threshold. For example, the examiner should consider whether the corporate will continue to maintain adequate capital levels in light of current and planned activities, such as Expanded Authorities.

Corporates operating at Base or Base-Plus Expanded Authority must maintain a minimum capital ratio of 4 percent. However, a corporate with Part I or II Expanded Authority will need a minimum 4, 5, or 6 percent capital ratio depending on their corresponding NEV exposure limit of 20, 28, or 35 percent, respectively. The examiner must keep in mind that these ratios are merely the minimum regulatory requirement; given additional risks in each corporate, these ratios may be minimally adequate or even inadequate.

As part of the risk rating process the examiner will assign a Financial Risk Component Rating to Empirical Capital Strength and a Risk Management Component Rating to Capital Accumulation Planning. The capital versus risk relationship will be reflected in the Overall Financial Risk Composite Rating when the Empirical Capital Level Component Rating is evaluated in relation to the other risk related components (i.e., interest rate, liquidity, credit, earnings risks).

Empirical Capital Level

In assigning this Component Rating, the examiner should consider all capital related Evaluation Factors and any additional issues directly or indirectly affecting capital. At a minimum, the following Evaluation Factors should be considered:

Retained Earnings Ratio:

Retained earnings and the retained earnings ratio are defined in Section 704.2. When assigning a risk ranking to this factor, the examiner should consider the corporate's overall level of financial and operational risks, including any Expanded Authorities. Generally, a corporate taking on higher degrees of credit, interest rate, liquidity, and operational risk should maintain a higher level of retained earnings, as noted in the table below:

Recommended Risk Rankings for Retained Earnings Evaluation Factor

Risk Ranking	Base, Base+	Part I	Part II
1	5.0% or greater	5.5% or greater	6.0% or greater
2	3.0 to less than 5.0%	3.5% to less than 5.5%	4.0% to less than 6.0%
3	2.0% to less than 3.0%	2.5% to less than 3.5%	3.0% to less than 4.0%
4	1.0% to less than 2.0%	1.5% to less than 2.5	2.0% to less than 3.0%
5	less than 1.0%	less than 1.5%	less than 2.0%

Note: Part III corporates are evaluated using the column corresponding with their Part I or Part II authority and NEV threshold. Part IV and V corporates are evaluated under the Base and Base+ column unless they have an expanded authority level requiring use of another column. Wholesale corporates are evaluated under the column for Part I authority.

Core Capital Ratio: When assigning the ranking for the core capital ratio (as defined in Section 704.2), the examiner will take into account the corporate's earnings retention position, and the trend and mix of capital.

Capital Ratio: Section 704.3 and Appendix B to Part 704 set forth specific capital ratio requirements for Base and each level of Expanded Authorities. As noted in Appendix B, the minimum capital ratio is also established as a result of the designated NEV exposure limit chosen by corporates with Part I or II Expanded Authorities. The examiner should consider the corporate's current capital level, and ability to achieve future capital goals when assigning the rating for this Evaluation Factor. The table below establishes the recommended risk rankings based on each corporate's Expanded Authorities or operating level:

Recommended Risk Rankings for Capital Ratio Evaluation Factor

Risk Ranking	Base & Base+	Part I 20% NEV	Part II 20% NEV	Part I 28% NEV	Part II 28% NEV	Part I 35% NEV	Part II 35% NEV
1	6.0% or greater	6.50% or greater	7.00% or greater	7.00% or greater	7.50% or greater	7.50% or greater	8.00% or greater
2	5.0% or less than 6.0%	5.50% or less than 6.50%	6.00% to less than 7.00%	6.00% to less than 7.00%	6.50% or less than 7.50%	6.50% or less than 7.50%	7.00% or less than 8.00%
3	4.0% or less than 5.0%	4.50% or less than 5.50%	5.00% or less than 6.00%	5.00% or less than 6.00%	5.50% or less than 6.50%	5.50% or less than 6.50%	6.00% or less than 7.00%
4	3.0% or less than 4.0%	3.50% or less than 4.50%	4.00% or less than 5.00%	4.00% or less than 5.00%	4.50% or less than 5.50%	4.50% or less than 5.50%	5.00% or less than 6.00%
5	Less than 3.0%	Less than 3.50%	Less than 4.00%	Less than 4.00%	Less than 4.50%	Less than 4.50%	Less than 5.00%
Note: Part III corporates are evaluated using the column corresponding with their Part I or Part II authority and NEV threshold. Part IV and V corporates are evaluated under the Base and Base+ column unless they have an expanded authority level requiring use of another column. Wholesale corporates are evaluated under the column for Part I authority.							

Capital Trends: When determining the Empirical Capital Component Rating, the EIC must consider the capital level, mix, and trends during as of the effective date of the examination. The EIC should also consider the risk rankings assigned to the above Evaluation Factors. The overall Financial Risk Composite Rating will reflect the relationship between Empirical Capital Strength and balance sheet and operational risk levels.

Capital Accumulation Planning Component Rating

As part of the examination process, the examiner will evaluate and assess the strength of the corporate's capital accumulation plan, and the effectiveness with which it is implemented. The capital accumulation plan should be developed after careful consideration of current and projected balance sheet and operational risk activities (i.e., Expanded Authorities, new services, etc.).

Capital accumulation plans will be evaluated and assigned a component rating that will be included in the derivation of the overall Risk Management Composite Rating. The evaluation of capital accumulation plans will require that the examiner draw upon a variety of other financial and risk related factors impacting the corporate. Chapter 204 of this guide provides detailed discussion of some of the attributes of effective capital accumulation planning.

Earnings and Profit Planning Component

A corporate should have earnings sufficient to accumulate capital levels to meet or exceed minimum capital requirements and absorb operating losses. The minimum capital requirements will vary in relation to Expanded Authorities, as well as the corporate's overall balance sheet and operational risk profile. Examiners should use professional judgment to evaluate the adequacy of earnings in relation to the level of capital and the risks inherent in the portfolio, and any off-balance sheet risks. For example, a corporate with Parts II and IV Expanded Authorities will be evaluated more stringently than one with Base-Plus Expanded Authority because it has the authority to expose its capital and earnings to greater risk.

When examiners assess the adequacy of corporate earnings, general economic and market related factors should be considered. Earnings trends and balance sheet flexibility are two factors that should be considered, in addition to actual financial results.

Given the complexity of each corporate's balance sheet, there is no easy formula for determining the adequacy of earnings. The examiner should look for earnings characteristics such as stability, trend, and composition. The level of operating expenses should be reviewed in relation to the overall earnings composition. The examiner should be cognizant of the risk/return tradeoff or concept often employed as part of corporate asset/liability management strategies. Generally, assets carrying additional risk should provide an adequate compensating return used to build capital, or to provide the membership with greater return.

Although the minimum capital requirements are specifically set forth in Section 704.3, and Appendix B to Part 704, the adequacy of earnings is subjective based on qualitative and quantitative factors and the examiner's professional judgment. These qualitative and quantitative measures may relate to, but are not limited to, the current capital level, the level of credit, interest rate, liquidity, and operational risk, and management's effectiveness. Further guidance for evaluating earnings is discussed in Chapter 302 of this guide.

When evaluating the adequacy of earnings, the examiner should consider the following factors:

<u>Quantitative Earnings Evaluation Factors (Financial Risk Composite)</u>

1. Net Income Level;
2. Earnings Trends;
3. Earnings Composition (gross income, cost of funds, fee income);
4. Operating Expenses;
5. Product Line Profitability; and

6. Non-Operating Income Level.

Qualitative Earnings Evaluation Factors (Risk Management Composite)

1. Budgeting and Reporting;
2. Earnings in Relation to Capital Planning;
3. Effectiveness of Cost Accounting Systems; and
4. Pricing Strategies and Policies.

Sensitivity to Interest Rate Risk

Interest rate risk (IRR) is the exposure of capital and earnings to movements in interest rates. The economic perspective, termed net economic value (NEV), focuses on the difference in the fair value of assets and the fair value of liabilities in today's interest rate environment and the sensitivity of NEV to interest rate changes. The accounting perspective, referred to as net interest income (NII), focuses on the effect of interest rate changes on the corporate's projected earnings under both current and projected interest rate scenarios.

The IRR Component Rating addresses the corporate's performance in identifying, measuring, monitoring, reporting, and controlling exposure to interest rate changes. The examiner will assess quantitative and qualitative factors in order to assign an Interest Rate Risk Exposure Component Rating and an Interest Rate Risk Management Component Rating, respectively.
Given the importance of each corporate's IRR management process, qualitative factors such as the robustness of the model and validity of the assumptions will be utilized in assigning both the quantitative and qualitative components.

In deriving the IRR Component Rating, the examiner is to consider 12 Evaluation Factors listed in this section. The examiner should determine whether rankings for additional factors are to be documented under the "other" caption.

The examiner should assign the component rating on a case-by-case basis using professional judgment, and will consider the interrelationships of the Evaluation Factors in light of any Expanded Authorities.

The Sensitivity/IRR Evaluation Factors focus the examiner on the sensitivity measures, documentation, and testing the

corporate performs, rather than on management's capabilities. The examiner's evaluation of management's effectiveness and expertise should be considered when assigning the IRR Management Component Rating under the overall Risk Management Composite.

Considering the interrelationships of the various Evaluation Factors, the examiner may assign a lower or higher ranking than is specified in the guidelines; however, the rationale or justification for such decisions should be well-documented in the examination work papers**.** The examiner should refer to Appendix 401A when assessing these Evaluation Factors.

Qualitative IRR Exposure Evaluation Factors

Base case NEV ratio: Under Section 704.8, a corporate must calculate its NEV ratio at least quarterly; the NEV ratio must be calculated monthly, if the NEV ratio falls below 3 percent at the last testing date. In general, corporates with Expanded Authorities must compute their NEV ratio monthly; however, the specific requirements are detailed in Appendix B to Part 704.

Section 704.8 establishes a minimum NEV ratio floor of 2 percent under the worst-case test for parallel shocks in the Treasury yield curve. Therefore, a 2 percent base case NEV ratio represents a weak capital position and an excessive risk level limiting the corporate's flexibility to respond to interest rate shocks and comply with the Section 704.8(d)(1)(ii) NEV Exposure Measure. Corporates in this situation have a very small margin for error with their NEV modeling process and even a slight increase in IRR jeopardizes their compliance with the 2 percent NEV ratio floor.

Examiners should compare each corporate's base NEV ratio, NEV Exposure Measure, and NEV Volatility Measure to the following tables to assist them in determining the overall IRR Component Rating:

BASE NEV RATIO			
Ranking	Base, Base +	Part I	Part II
1	6.0% or greater	6.5% or greater	7.0% or greater
2	5.0% to 5.99%	5.5% to 6.49%	6.0% to 6.99%
3	4.0% to 4.99%	4.5% to 5.49%	5.0% to 5.99%
4	3.0% to 3.99%	3.5% to 4.49%	4.0% to 4.99%
5	Less than 3.0%	Less than 3.49%	Less than 3.99%

NEV Exposure Measure (worst case NEV ratio): Section 704.8(d)(1)(ii) provides that a corporate must limit its risk exposure to a level that does not result in an NEV ratio below 2 percent under parallel shocks in the yield curve of plus/minus 300 basis points. Generally, a low risk corporate would maintain an NEV Exposure Measure above 3 percent, as noted below.

NEV EXPOSURE MEASURE	
Ranking	All Authorities
1	5.0% or greater
2	4.0% to 4.99%
3	3.0% to 3.99%
4	2.0% to 2.99%
5	Less than 2.0%

NEV Volatility Measure (post shock percentage change in NEV ratio): This factor is defined in Section 704.2. The corporate must limit its IRR exposure under parallel shocks in the yield curve across a range of plus/minus 300 basis points to a level that does not result in an NEV Volatility Measure of more than 15, (Base), 20 (Base+), 20, 28, or 35 for corporates having Part I and/or II Expanded Authority. Refer to the tables below.

NEV VOLATILITY MEASURE		
Ranking	15% NEV Limit	20% NEV Limit
1	less than 6.0%	less than 9.0%
2	6.0% to less than 9.99%	9.0% to 14.99%

3	10.0% to 14.99%	15.0% to 19.99%
4	15.0% to 19.99%	20.0% to 27.99%
5	20.0% or greater	28.0% or greater

NEV VOLATILITY MEASURE		
Ranking	**28% NEV Limit**	**35% NEV Limit**
1	less than 12.0%	less than 15.0%
2	12.0% to 19.99%	15.0% to 24.99%
3	20.0% to 27.99%	25.0% to 34.99%
4	28.0% to 34.99%	35.0% to 39.99%
5	35.0% or greater	40.0% or greater

Qualitative IRR Management Evaluation Factors

Risk Model Capabilities: This Evaluation Factor reflects the examiner's conclusions regarding the capabilities of the NEV model as implemented by management or a third-party vendor (i.e., if NEV modeling is outsourced). The examiner should refer to Chapter 202, Asset/Liability Management, and to corporate staff for documentation of the fundamental characteristics of the risk model. The examiner should document any overrides of industry standard inputs indigenous to NEV modeling.

Modeling Assumptions: This Evaluation Factor considers whether the price sensitivities are reasonable and supportable in light of any prepayment speed assumptions. The examiner will consider the source (such as information vendor or in-house systems) of prepayment estimates used to measure and monitor the price sensitivity of complex investments. If the model generates securities valuation output at the individual instrument level, such detail may serve as appropriate evidence of securities price sensitivity monitoring.

Additional NEV and Stress Testing

The examiner should assess the frequency, accuracy, and validity of the additional tests periodically required by Section 704.8(d)(2). This assessment should include determining whether management should go above and beyond the regulatory requirements, based on balance sheet risk, or external factors (i.e., interest rate environments, economic conditions, event risk, etc.). For example, performing rate shocks of 400 or 500 basis points, ramped simulations, etc. Consideration should also be given to the corporate's Expanded Authority level when assessing whether the frequency and scope of additional testing are adequate.

Modeling Process/Internal Control: The examiner should assess the reasonableness of the modeling process, including the audit trail, and the change control process (i.e., a change of algorithm or a change of source of volatility, etc.).

ALCO Documented Strategies: The examiner should review ALCO's documented strategies and assess whether balance sheet changes have been consistent with those strategies. The examiner may consider documented changes in strategies and changes in market conditions in assigning this ranking.

Compliance, Including Internal Validation: The examiner should review the corporate's documentation of its compliance with internal policy limits and with Section 704.8 requirements.

Third Party Validation: The examiner should review any third party validation for scope, methodology, and reasonableness, as required by Section 704.4.

Policies/Procedures: The examiner should review any IRR policies and procedures to determine whether material omissions or deficiencies exist.

Other: The EIC should assign other evaluation factors in light of individual circumstances and any Expanded Authorities.

Liquidity Risk Exposure and Management

Liquidity Risk is the exposure of capital and earnings to costs incurred by the corporate in meeting present and anticipated cash flow needs. Liquidity Risk generally arises from potential mismatches between asset and liability cash flows. Liquidity Risk assessment is complicated by the uncertainties of asset and liability cash flows due to embedded options or other derivatives impacting cash flows. Liquidity Risk includes the risk of early and unexpected share account redemptions.

Liquidity Risk Management includes assessing the memberships’ potential liquidity needs in a variety of economic scenarios. Reference should be made to Section 704.9 (Liquidity), and Chapter 202 (ALM) of this guide for further liquidity related factors.

Liquidity sources typically include advised and committed LOCs from U.S. Central or other institutions repurchase transactions, security sales, and commercial paper. The examiner should assess the corporate’s analysis of assets to determine the degree of marketability and potential use of assets as collateral to provide liquidity in the event that this option becomes necessary and is cost beneficial. The examiner should assess the corporate’s analysis of the behavior of its shares under normal and alternative economic scenarios, including under a stress (“worst-case”) scenario. Management’s analysis of the potential liquidity impact arising from any off-balance sheet activities is also a factor.

In measuring and managing net funding requirements, a corporate should prepare a schedule comparing future cash inflows to outflows over a series of time periods. The difference between cash inflows and outflows in each period, or the excess or deficit of funds, becomes a starting-point for a measure of a corporate’s future liquidity excess or shortfall. The assessment of different economic scenarios should provide a basis for the corporate’s plans to fill any liquidity shortfalls. The examiner should assess the adequacy of the cash flow related assumptions under different scenarios.

The examiner should assess the corporate’s access to external (market) sources of liquidity. This assessment should include a review of the diversification of its liabilities, the documented established relationships with liability-holders (e.g., commercial paper), and the corporate’s asset-sales markets, if any. Building strong relationships with funding sources can provide a corporate with additional options in the event that contingency liquidity plans need to be implemented. The frequency of contact with and use of a funding source are two indicators of the strength of a funding relationship.

At a minimum, the following Quantitative and Qualitative Liquidity Risk Evaluation Factors should be reviewed:

Quantitative Liquidity Risk Evaluation Factors

1. Significant asset/liability concentrations;
2. Core funds determination; and
3. Liquidity measures - cash budgeting.

Qualitative Liquidity Management Evaluation Factors

1. Policies/Procedures (i.e., objectives and contingency plans);
2. Alternative Funding Sources:
    a. Development.
    b. Maintaining market presence.
    c. Testing.
    d. Commercial Paper.
    e. Repurchase opportunities;
3. Disintermediation plan (worse case);
4. Early withdrawal penalties;
5. Compliance/monitoring; and
6. Other relevant factors.

Credit Risk

Credit risk is present any time a corporate extends credit, purchases investments, makes commitments and guarantees, and enters into contractual agreements, whether reflected on or off balance sheet. In other words, credit risk is found in all activities where success depends on counterparty, issuer, or a borrower's ability to perform or repay.

Credit risk arises when engaging in a broad range of activities including, the selection of investment products, brokers, and counterparties. Credit risk also arises due to country or sovereign exposure, as well as indirectly through guarantor performance. These credit risks are discussed in more detail in Chapters 201, Investments and 203, Loan Review.

When rating credit risk, the examiner should consider both the quantitative level of credit risk the corporate is exposed to (i.e., concentration risks, third party credit ratings of investment securities, etc.), as well as qualitative factors (i.e., credit risk management policies and procedures). At a minimum, the following key factors should be evaluated when determining Credit Risk Exposure and Credit Risk Management Component Ratings:

Quantitative Credit Risk Exposure Evaluation Factors (Financial Risk Composite)

1. Concentrations of credit by investment type;
2. Concentrations of credit by issuer;
3. Concentrations by sector or industry;
4. Concentrations of loan commitments and/or guarantees; and
5. Loan delinquency and charge off ratios and trends.

Qualitative Credit Risk Management Evaluation Factors (Risk Management Composite)

1. Quality of investment, loan, and credit risk management policies and procedures;
2. Quality of loan underwriting;
3. Quality of credit administration, documentation, and reporting (securities, counterparties, credit ratings, watch lists, outstanding commitments, and ongoing monitoring);
4. Quality of assets; and
5. Other applicable credit risk factors.

The examiner must tailor the scope of the credit risk management review to the corporate's Part 704 Expanded Authority level. For example, a corporate with Base operating authority and a relatively simple investment portfolio will not be expected to have an extremely sophisticated credit risk management function. However, corporates with Part I or II Expanded Authorities can purchase lower rated investments requiring a more elaborate credit risk management process. Specifics related to the credit review required for the various Expanded Authorities are discussed in Chapter 201, Investments, and in the Guidelines for Submission of Requests for Expanded Authority.

Operations, Board Oversight, Audit and Compliance

Management consists of the board of directors, various committees, and operating management. The quality of management is the most important element in the successful operation of a corporate. The quality of this element is normally the factor most indicative of how well risk is identified, measured, monitored, reported, and controlled.

Strong management is a key factor in a corporate remaining financially sound, regardless of external factors. External factors include items such as event risk, economic conditions, interest rate environments, and other factors impacting the corporate's balance sheet or financial condition. The ability to promptly address existing problems and risks, and the capacity to be forward thinking, contribute to the success of each corporate, and help ensure membership obligations are continuously met.

Management's expertise level must be commensurate with its current and projected risk activities. Specific capabilities of officials and operating management will be evaluated and ranked when reviewing the risk management process established for various risk activities.

When assigning the component ratings to Operations and Board Oversight, Audit & Compliance, the examiner will draw upon the analysis of various qualitative risk factors. This process will provide an assessment of the officials overall ability to effectively identify, measure, monitor, report, and control each of the numerous risks inherent in the corporate's operation. Other less tangible or measurable aspects of the management function will be reviewed and risk ranked under the component Evaluation Factors listed below. The examiner should refer to various chapters of this guide when assessing the quality of specific managerial and operational functions.

The following Evaluation Factors should be considered in conjunction with the Expanded Authorities under which the corporate operates (if applicable). The assessment of management's performance under each of these Evaluation Factors is used to determine the overall Operations and Board Oversight, Audit & Compliance Component Ratings.

Operations Component Rating

1. Overall completeness of documented procedures for all operational areas;
2. Adequacy of internal controls for all operational areas;
3. Adequacy of management of MIS systems risk including the LAN, wires, ACH, and item processing; and
4. Other evaluation factors as applicable.

Board Oversight, Audit and Compliance Component

1. Management's overall strategic planning process;
2. Appropriateness and completeness of succession planning;
3. Management's ability to attract and retain sufficiently qualified and experienced personnel;
4. Quality of policy and procedure making activities for all operational areas;
5. Adequacy of continuing education and training for the board, committees, and staff;
6. Effectiveness of the board, committees, and staff;
7. Independence and effectiveness of compliance function;
8. Response to supervision;
9. Accuracy of financial reporting and accounting functions;
10. Response to the internal and external audit functions;
11. Extent of cross training and backup processes;
12. Adequacy and effectiveness of the corporate's infrastructure;
13. Management's effectiveness in addressing legal matters;
14. Effective use of consultants, vendors, and outsourcing; and
15. Other evaluation factors as applicable.

Both the Operations and Board Oversight, Audit & Compliance Component Ratings are qualitative. The overall evaluation of management effectiveness and internal controls does incorporate many of the underlying quantitative factors of the other risk management components, as well as internal, operational, and system controls for corporate operations.

When considering the assignment of risk rankings to the above Evaluation Factors, the examiner should refer to applicable sections of this guide, Part 704, and the Guidelines for Submission of Requests for Expanded Authorities.

Examination Objectives

The EIC's assignment of CRIS Composite Ratings culminates an examination team's review of all significant financial, operational, and compliance evaluation factors in a corporate.

The examination objectives in assigning a CRIS Rating are to:

1. Reflect the weaknesses and corrective actions noted in the examination report;

2. Communicate the EIC's overall assessment of the corporate's condition and viability to NCUA; and

3. Disclose to management NCUA's overall assessment of the corporate's Financial Risk and Risk Management abilities.

Supervision

Supervision provided to individual corporates will be based upon the asset size, Expanded Authority level, and the CRIS Composite Ratings. Supervision plans are developed by the EIC with the concurrence of the CFS and the OCCU Director as discussed in Chapter 102 of this guide.

Examination Procedures

See Corporate Examination Procedures - CRIS (OCCU 401P).

Appendices

Appendix 401 A - CRIS Composite and Component Rating Definitions & Evaluation Factors

Appendix 401A

CRIS COMPOSITE AND COMPONENT RATING DEFINITIONS AND EVALUATION FACTORS

FINANCIAL RISK COMPOSITE RATING

The Financial Risk Composite Rating is based on a careful evaluation of a corporate's financial performance. The five key components used to assess an institution's financial strength are empirical capital measures, credit risk exposure, interest rate risk exposure, liquidity risk exposure, and level and composition of earnings.

The composite rating scale ranges from 1 to 5, with a rating of 1 indicating the strongest level of financial performance relative to the institution's complexity, risk profile, and approved expanded authorities (as applicable); and the level of least supervisory concern. A rating of 5 indicates a critically deficient level of financial performance and an excessive risk profile given approved expanded authorities (as applicable); and the greatest supervisory concern. The composite ratings are defined as follows:

1. Corporate credit unions in this group exhibit a strong financial condition in every respect and generally have financial risk component ratings of 1 or 2. Any financial weaknesses are minor and can be corrected or improved in a routine manner by the board of directors and management. These corporate credit unions are the most capable of withstanding economic instability and market interest rate fluctuation. These corporates are in compliance with all regulations pertaining to the accumulation of capital and management of interest rate, credit, and liquidity risks. As a result, these corporate credit unions exhibit the strongest financial performance and risk profile relative to the complexity of operations and approved expanded authorities (as applicable).

2. Corporate credit unions in this group are fundamentally sound. For a corporate to receive this rating, no component rating will be more severe than 3. Only moderate financial weaknesses are present and are well within the board of directors' and management's capabilities and willingness to correct. These corporate credit unions are stable and are capable of withstanding business fluctuations. These corporate credit unions are in substantial compliance with all regulations pertaining to the accumulation of capital and management of interest rate, credit, and liquidity risks. Risk exposures are acceptable relative to the complexity of the corporate's operations and expanded authorities granted (if applicable).

3. Corporate credit unions in this group exhibit a degree of supervisory concern in one or more of the component areas. These corporates exhibit a combination of financial weaknesses that may range from moderate to severe; however, the individual components are not rated more severely than 4. Corporate credit unions in this group generally are less capable of withstanding business fluctuations and are more vulnerable to outside influences than those corporates rated a composite 1 or 2. These corporates may be in significant noncompliance with regulations pertaining to the accumulation of capital and management of interest rate, credit, and liquidity risks. The overall risk profile of the corporate is less than satisfactory relative to the complexity of operations, and expanded authorities granted (if applicable).

4. Corporate credit unions in this group generally exhibit serious financial deficiencies that result in unacceptable performance. The problems range from severe to critically deficient. Corporate's in this group are generally not capable of withstanding business fluctuations. There may be significant noncompliance with regulations pertaining to the accumulation of capital and management of interest rate, credit, and liquidity risks. The corporate's overall risk profile is unacceptable relative to the complexity of operations and expanded authorities granted (if applicable). Institutions in this group pose a risk to the National Credit Union Share Insurance Fund (NCUSIF).

5. Corporate credit unions in this group exhibit critically deficient performance and risk profiles relative to the complexity of operations and expanded authorities granted (if applicable). The volume and severity of problems are beyond the board and management's ability or willingness to control or correct. Immediate NCUSIF financial or other assistance is needed in order for the corporate to be viable. Continual supervisory attention is necessary. Institutions in this group pose a significant risk to the NCUSIF and failure is highly probable.

RISK MANAGEMENT COMPOSITE RATING

The Risk Management Composite Rating is based on a careful evaluation of a corporate’s risk management policies, practices, and expertise. The seven key components used to assess an institution’s financial strength are: Capital Accumulation and Planning, Profit Planning and Control, Interest Rate Risk Management, Liquidity Risk Management, Credit Risk Management, Board Oversight Audit & Compliance, and Operations.

The rating scale ranges from 1 to 5. A rating of 1 indicates: the highest quality risk management, operational, and supervisory practices relative to the institution’s complexity, risk profile, and approved expanded authorities; and the level of least supervisory concern. A rating of 5 indicates: a critically deficient quality of risk management, operational, and supervisory practices given approved expanded authorities; and the greatest supervisory concern. Composite ratings are defined as follows:

1. A rating of 1 indicates strong performance by management and the board of directors and strong risk management practices relative to the corporate’s authorities granted under Part 704. All significant risks are consistently and effectively identified, measured, monitored, and controlled. Management and the board have demonstrated the ability to promptly and successfully address existing and potential problems and risks.

2. A rating of 2 indicates satisfactory management and board performance and risk management practices relative to the corporate’s authorities granted under Part 704. All operational policies and practices are deemed fundamentally sound. Minor weaknesses may exist, but are not material to the safety and soundness of the corporate and are being addressed.

3. A rating of 3 indicates management and/or board performance that requires improvement, or risk management practices that are less than satisfactory given the corporate’s expanded authorities under Part 704. The capabilities of management or the board of directors may be insufficient for this corporate. Financial and/or operational problems and significant risks may be inadequately identified, measured, monitored, or controlled.

4. A rating of 4 indicates deficient management and/or board performance or risk management practices that are inadequate considering the corporate's expanded authorities under Part 704. The levels of financial and/or operational problems and risk exposures are excessive. Financial and/or operational problems and significant risks are inadequately identified, measured, monitored, or controlled and require immediate board and management action to preserve the corporate's soundness.

5. A rating of 5 indicates critically deficient management and board performance or risk management practices. Management and/or the board of directors have not demonstrated the ability to correct financial and/or operational problems and implement appropriate risk management practices. Financial and/or operational problems and significant risks are inadequately identified, measured, monitored, or controlled and now threaten the continued viability of the corporate.

INDIVIDUAL FINANCIAL RISK AND RISK MANAGEMENT COMPONENT RATINGS

Empirical Capital Measure Component Ratings

A rating of 1 indicates a strong capital level. No negative trends are apparent.

A rating of 2 indicates a satisfactory capital level. Some negative trends may be apparent; however, the retained earnings and capital ratios meet or exceed the minimum regulatory requirements. Generally, the corporate is not approaching a capital position that will require either an earnings retention requirement, under Section 704.3(i), or a capital restoration plan under Section 704.3(g).

A rating of 3 indicates retained earnings and capital ratios meet or exceed the minimum regulatory requirements of Section 704.3(i) and Section 704.3(d); however, the rating indicates that the capital position is approaching a level where either earnings retention, under Section 704.3(i), or a capital restoration plan, under Section 704.3(g), will be required.

A rating of 4 indicates either the retained earnings and/or capital ratios are less than the minimum regulatory requirements of Sections 704.3(i) and 704.3(d), as applicable. Indications are the corporate will be subject to either Section 704.3(i) and/or a capital restoration plan for some time.

A rating of 5 indicates a critically deficient level of capital such that the corporate credit union's viability is threatened.

Capital Accumulation Planning Component Ratings

A rating of 1 indicates that the corporate has set forth reasonable plans for the continued maintenance or accumulation of capital in relation to other financial and operational risks incurred by the corporate, and has consistently achieved the objectives set forth in those plans.

A rating of 2 indicates that the corporate has set forth reasonable plans for the continued maintenance or accumulation of capital in relation to other financial and operational risks incurred by the corporate, and has normally achieved the goals set forth in those plans.

A rating of 3 indicates that capital accumulation plans set forth by management are weak in relation to the financial and operating risks incurred by the corporate, and goals and objectives set forth in those plans are frequently not achieved.

A rating of 4 indicates that capital accumulation plans either are non-existent, or seriously deficient in relation to the corporate's current capital level, financial and operational risks.

A rating of 5 indicates that corporate management is either unwilling or incapable of developing and implementing effective capital accumulation plans putting the future solvency of the institution in jeopardy.

Earnings and Profitability Component Ratings

A rating of 1 indicates strong earnings. Earnings are more than sufficient to support operations and to accumulate adequate reserves and undivided earnings after considering credit risk, liquidity risk, interest rate risk, growth, composition of income and expense, and other factors affecting the quality, quantity, and trend of earnings.

A rating of 2 indicates the level of earnings is satisfactory. Earnings are sufficient to support operations and maintain the accumulation of adequate reserves and undivided earnings after considering credit risk, liquidity risk, interest rate risk, growth, composition of income and expense, and other factors affecting the quality, quantity, and trend of earnings. Earnings that are relatively static, or even experiencing a slight decline, may receive a 2 rating provided the corporate credit union's level of earnings is adequate in relation to the core capital and retained earnings ratios.

A rating of 3 indicates a level of earnings that needs improvement. Earnings may not fully support operations and provide for retained earnings growth commensurate with asset growth after considering credit risk, liquidity risk, interest rate risk, composition of income and expense, and other factors affecting the quality, quantity, and trend of earnings.

A rating of 4 indicates a level of earnings that is deficient. Earnings are insufficient to maintain appropriate retained earnings. Corporate credit unions so rated may be characterized by erratic fluctuations in net income or net interest margin, the development of significant negative trends, nominal or unsustainable earnings, intermittent losses, or a substantive drop in earnings from previous reporting periods.

A rating of 5 indicates earnings that are critically deficient. A corporate credit union with earnings rated 5 is experiencing losses that represent a distinct threat to its viability through the erosion of capital.

Profit Planning and Control Component Ratings

A rating of 1 indicates that management has set forth a reasonable and accurate budgeting and cost accounting process that allows for the effective management of fee income and operating expenses in relation to net-interest margin, asset growth, and capital accumulation objectives. Budgeted goals and objectives are consistently obtained with no major variances or revisions to projections are required.

A rating of 2 indicates that management has set forth a reasonable and accurate budgeting and cost accounting process that enable the effective management of fee income and operating expenses in relation to net-interest margin, asset growth, and capital accumulation objectives. Budgeted goals and objectives are normally obtained. Minor variances and revisions are sometimes incurred.

A rating of 3 indicates that management's budgeting and cost accounting processes are weak and normally ineffective in measuring, monitoring, and controlling corporate earnings.

A rating of 4 indicates that management's budgeting and cost accounting processes are unreasonable, inaccurate, and critically deficient in measuring, monitoring, and controlling corporate earnings.

A rating of 5 indicates that management is unwilling or unable to develop and implement effective budgetary and cost accounting systems.

Interest Rate Risk Exposure Component Ratings

A rating of 1 indicates that NEV is strong and well controlled and that there is minimal potential that financial performance will be adversely affected or regulatory requirements will be violated. The level of earnings and the NEV ratio provide substantial support for the degree of market risk taken by the corporate credit union.

A rating of 2 indicates that interest rate sensitivity is acceptable and adequately controlled. There is only moderate potential that financial performance will be adversely affected or regulatory requirements will be violated.
A rating of 3 indicates that control of interest rate exposure needs improvement or that there is significant potential that the NEV ratio will be in violation of the regulatory limits of Section 704.8, or the applicable part of Appendix B of Part 704. The level of earnings and the NEV ratios may not adequately support the degree of NEV exposure.

A rating of 4 indicates that the corporate's interest rate sensitivity is in violation of the regulatory limits of Section 704.8, or the applicable part of Appendix B of Part 704. The NEV or NEV ratio reflect an immediate need to plan and take action to restructure the balance sheet to bring the corporate into compliance.

A rating of 5 indicates a corporate's interest rate sensitivity is in violation of the regulatory limits of Section 704.8, or the applicable part of Appendix B of Part 704. The level of risk is unacceptable and/or an imminent threat to the corporate's viability.

Interest Rate Risk Management Component Ratings

A rating of 1 indicates that interest rate risk management practices are strong for the expanded authorities approved (if applicable), sophistication, and level of interest rate exposure of the corporate. No weaknesses are noted, and no supervisory concerns exist.

A rating of 2 indicates that interest rate risk management practices are satisfactory for the expanded authorities approved (if applicable), sophistication, and level of interest rate exposure of the corporate. Some minor weaknesses may be noted with limited supervisory concern.

A rating of 3 indicates that interest rate risk management practices need to be improved given the expanded authorities approved (if applicable), sophistication, and level of interest rate exposure of the corporate. Major weaknesses are noted, and a high degree of supervisory concern exists regarding the adequacy of interest rate risk management policies and practices.

A rating of 4 indicates that interest rate risk management practices are deficient under any expanded authorities approved (if applicable). Severe weaknesses are noted. Management lacks the expertise to set forth appropriate risk management strategies and practices, and major supervisory concerns exist regarding the adequacy of interest rate risk management polices and practices and regulatory intervention may be necessary.

A rating of 5 indicates that interest rate risk management practices are wholly inadequate for the authority, sophistication, and level of interest rate exposure of the corporate. Critical deficiencies are noted. Management lacks the willingness and expertise to set forth appropriate risk management strategies and practices. Supervisory intervention is required.

Liquidity Risk Exposure Component Ratings

A rating of 1 indicates strong liquidity levels and reliable access to sufficient sources of funds on favorable terms to meet present and anticipated liquidity needs.

A rating of 2 indicates satisfactory liquidity levels and funds management practices. The corporate has access to sufficient sources of funds on acceptable terms to meet present and anticipated liquidity needs.

A rating of 3 indicates a weak level of liquidity in relation to short- and long-term cash funding needs. Corporates rated 3 may lack ready access to funds on reasonable terms or may evidence significant weaknesses in funds management practices.

A rating of 4 indicates deficient liquidity levels, and the need for frequent borrowing to fund daily cash needs. Corporates rated 4 may not have, or be able to obtain, a sufficient volume of funds on reasonable terms to meet liquidity needs.

A rating of 5 indicates liquidity levels or funds management practices so critically deficient that the continued viability of the corporate is threatened. Corporates rated 5 require immediate external financial assistance to meet maturing obligations or other liquidity needs.

Liquidity Risk Management Component Ratings

A rating of 1 indicates that liquidity management policies and practices are strong. Management has developed and maintained reasonable and accurate processes to measure, monitor, and control short- and long-term access to funds. Effective policies have been set forth that identify effective liquidity contingency plans. No supervisory concerns are noted.

A rating of 2 indicates that liquidity management policies and practices are adequate. Management has developed and maintained processes to measure, monitor, and control short- and long-term access to funds. Liquidity contingency plans have been developed. Some minor weaknesses in these plans, policies, and practices may be noted. Some minor supervisory concerns may be noted.

A rating of 3 indicates that liquidity management policies and practices are weak. Management's policies and processes for measuring, monitoring, and controlling short- and long-term access to funds may be unreasonable or inaccurate. There is normally a lack of sufficient liquidity contingency plans in place. A high degree of supervisory concern exists.

A rating of 4 indicates that liquidity management policies and practices are deficient. Management may lack the appropriate expertise to develop and maintain reasonable and effective processes to measure, monitor, and control short- and long-term access to funds. Major supervisory concerns exist.

A rating of 5 indicates that liquidity management policies and practices are critically deficient. Management lacks the ability and willingness to set forth appropriate liquidity management strategies, and regulatory intervention is necessary.

Credit Risk Exposure Component Ratings

A rating of 1 indicates a low level of credit risk exposure with respect to the corporate capital and regulatory requirements. No supervisory concern is noted.

A rating of 2 indicates a satisfactory level of credit risk exposure with respect to capital and regulatory requirements. Some concentrations, watch list assets, and other credit weaknesses may exist. However, only minor supervisory concern exists.

A rating of 3 indicates a high degree of credit risk exposure. There may be a significant level of concentrations, watch lists assets, and other credit weaknesses apparent. The severity of these risks requires an elevated level of supervisory concern.

A rating of 4 indicates the corporate's assets have a deficient level of credit quality. Significant credit concentrations, watch list assets, and other credit risks are apparent that may subject to the corporate to potential losses and threaten its viability. Major supervisory concerns exist.

A rating of 5 indicates a severely high degree of credit risk. Losses have been incurred due to these weaknesses, and the viability of the corporate is threatened. Major supervisory concern and follow up is required.

Credit Risk Management Component Ratings

A rating of 1 indicates strong credit analysis practices. The expertise of management and staff and sophistication of policies and practices are commensurate with approved expanded authorities (if applicable). Credit risk is of minimal supervisory concern.

A rating of 2 indicates satisfactory credit administration policies and practices commensurate with approved expanded authorities (if applicable). Some minor weaknesses may be noted; however, management has demonstrated the ability and willingness to correct them in an expedient and effective manner. Only limited supervisory concern is required.

A rating of 3 indicates administration practices that are less than satisfactory, considering the corporate credit union's expanded authority (as applicable). There is generally a need to improve credit administration practices, and management has been slow to initiate improvement. Moderate supervisory concern is required.

A rating of 4 indicates a corporate with deficient credit administration practices under base or any expanded authority level. There is a definite need to improve credit administration practices, and management may not possess the necessary expertise to do so. Major supervisory concern and follow up is required.

A rating of 5 indicates critically deficient credit administration practices. The corporate may have significant exposures that threaten viability. Management is unwilling and unable to initiate improvement and regulatory intervention is required.

Board Oversight, Audit & Compliance Component Ratings

A rating of 1 indicates strong board, committee, and management oversight. Effective managerial polices and procedures are evident in all areas of operation. Effective succession and backup plans are in place. Appropriate position descriptions and responsibilities have been set, and management and staff continually receive relevant and effective education to enable them to effectively meet the responsibilities of those positions. The corporate has an active and effective audit and compliance program, commensurate with expanded authorities granted. No supervisory concerns exist.

A rating of 2 indicates satisfactory board, committee, and management oversight. Effective managerial polices and procedures are in place for material areas of operation. Some minor weaknesses may be noted. The officials have set forth succession and backup plans that are either completely adequate or exhibit only minor weaknesses.

Position descriptions and responsibilities have been set forth, and management and staff generally receive relevant and effective education to enable them to meet their responsibilities. The corporate has a satisfactory audit and compliance program, commensurate with expanded authorities granted (if applicable). In some cases only minor audit and compliance related weaknesses will be noted. Management is responsive to audit and supervision efforts and addresses any deficiencies noted in a timely and effective manner. Only minor supervisory concern exists.

A rating of 3 indicates that one or more of these weaknesses are apparent. There is generally weak board, committee, and management oversight. Managerial polices and procedures are not in place for material areas of operation. Weaknesses are noted in policies that do exist. The officials have either not set forth succession and backup plans, or the plans are considered unreasonable and ineffective. Position descriptions and responsibilities have not been set forth, and management and staff generally do not receive relevant and effective education to enable them to effectively meet their responsibilities. The corporate's audit and compliance program may be unsatisfactory commensurate with expanded authorities granted (if applicable). Management may not be responsive to audit and supervision efforts. Major supervisory concern exists.

A rating of 4 indicates serious managerial weaknesses. The board, committees, and senior management have demonstrated an inability to set forth adequate infrastructure and organizational policy and practice. Critical supervisory concern exists.

A rating of 5 indicates critically deficient management oversight. The board, committees, and senior management are unwilling and unable to address organizational weaknesses. Regulatory intervention is required.

Operations Component Ratings

A rating of 1 reflects high quality operational policies, procedures and processes. Management's abilities, procedures, and practices are of minimal supervisory concern.

A rating of 2 reflects acceptable operational policies, procedures, and processes. Some minor weaknesses may be noted that management is willing and able to correct in an effective and efficient manner. Management's abilities, procedures, and practices warrant only a limited level of supervisory attention.

A rating of 3 reflects a moderate degree of weakness. Management's abilities, operational policies, procedures, and processes are less than satisfactory. The severity of these weaknesses and risks require an elevated level of supervisory review. There is a general need to improve management infrastructure and/or operational policies and practices.

A rating of 4 reflects serious deficiencies with respect to management's abilities, operational policies, procedures, and processes. The unsatisfactory nature of abilities, polices, procedures, and practices have put the assets of the corporate, members, and the NCUSIF at a high level of risk of financial loss or interruption of service. There is a definite need to improve the quality of policies and practices. Extensive supervisory attention is warranted.

A rating of 5 reflects critical deficiencies with respect to management's abilities, operational policies, procedures, and practices. The unsatisfactory nature of policies and practices may have caused financial losses, and threatens the viability of the institution. Management is unwilling and unable to take effective corrective action.

CORPORATE RISK IDENTIFICATION SYSTEM (CRIS)

Listing of CRIS Evaluation Factors by Component

Empirical Capital Component Ratings

Quantitative Empirical Capital Measures

Retained Earnings Ratio
Core Capital Ratio
Capital Ratio
Trends
- Ratio
- Dollars

Other

Qualitative Factors (i.e. Capital Accumulation Planning)

Reasonableness of Capital Accumulation Plan in Relation to Current Capital Levels and Risk Profile.

Earnings Component Ratings

Quantitative Earnings Measures

NI Level
Trends
Composition
- Gross Income
- Cost of Funds
- Fee Income
- Operating Expenses

Other

Qualitative Profit Planning and Management Factors

Budgeting and Reporting
Earnings in Relation to Capital Plans
Effectiveness of Cost Accounting Systems and Product Profitability
Pricing Strategies and Policies
Other

Interest Rate Risk Component Ratings

Quantitative Interest Rate Risk Exposure Measures
NEV Base Ratio
NEV Exposure Measure (worst case scenario relative to regulatory floor)
NEV Volatility Measure (change)
Other

Qualitative Interest Rate Risk Management Evaluation Factors
Robustness of Net Economic Value Simulation Models
Robustness of Net Interest Income Simulation Models
Additional NEV and Stress Testing
Expertise of Management and Staff - Interest Rate Risk Management
Modeling Process / Internal Control
ALCO Documented Strategies
Compliance Program and Third Party Validation (if applicable)
Policies/Procedures
Other

Liquidity Component Ratings

Quantitative Liquidity Risk Exposure Evaluation Factors

Concentration Risks
Reasonableness of Core Funds Determination
Liquidity Measures - cash budgeting
Other:

Qualitative Liquidity Risk Management Evaluation Factors

Policies / Procedures
- Objectives
- Contingency Plans

Alternative Funding Sources
- Development
- Maintaining Market Presence
- Testing
- CP
- Repo

Existence of Disintermediation Plan
Existence and Reasonableness of Early Withdrawal Penalties
Compliance / Monitoring
Other

Credit Risk Component Ratings

Quantitative Credit Risk Exposure Evaluation Factors

Concentrations of Credit by Investment Type
Concentrations of Credit by Issuer
Concentrations of Lending, Commitments and Guarantees
Third Party Credit Ratings
Other

Qualitative Credit Risk Management Evaluation Factors

Quality of Credit Risk Management Policies (Investments and Loans)
Quality of Credit Risk Management Procedures (written)
Quality of Loan Underwriting Practices
Quality of Credit Administration, Documentation, and Reporting (Investments)
Quality of Assets
Other

Board Oversight, Audit & Compliance Component Rating

Overall strategic planning process
Appropriateness and completeness of succession planning
Ability to attract and retain sufficiently qualified and experienced personnel
Quality of policy-making activities in all areas of operations and at all levels of management
Overall adequacy and effectiveness of the corporate's infrastructure
Overall effectiveness of the board of directors
Overall effectiveness of committees
Overall effectiveness of senior management;
Independence and effectiveness of compliance functions
Responsiveness to supervision
Sufficiency of and response to the internal audit function
Sufficiency of and response to the external audit
Extent of cross training and backup
Adequacy of continuing education and training for officials, senior management, and staff
Effectiveness in addressing legal matters
Effective use of consultants
Effective use of vendors and outsourcing
Other evaluation factors as applicable

Operations Component Rating

Overall completeness of documented procedures for all areas of operations
Accuracy of financial reporting and accounting functions
Adequacy of internal controls in all areas of operations
Adequacy of management of MIS systems risk including the LAN, wires, ACH, and item processing
Other evaluation factors as applicable

NATIONAL CREDIT UNION ADMINISTRATION CORPORATE EXAMINER'S GUIDE

The Corporate Examiner's Guide (CEG) provides guidance to National Credit Union Administration (NCUA) examiners for performing examinations and supervision of corporate credit unions. The primary goal is to ensure the overall safety and soundness of the corporate credit union system. While the CEG is intended to provide guidance to examiners, it also offers information that corporate credit unions may find useful in understanding the examination and supervision process.

Both state and federal examination staff examine corporate credit unions, depending upon whether the individual corporate is state or federally chartered. Federal examiners normally consist of staff from NCUA's Office of Corporate Credit Unions (OCCU). The OCCU uses a risk-focused examination and supervision process, which emphasizes ensuring corporate credit union management, identifies, measures, monitors, reports, and controls current and projected risk from their operations.

Although the guidance provided in this CEG is dependable, it may not necessarily be the best or final approach in every situation. The risk-focused examination approach requires examiners to exercise their professional judgment to assess the risk inherent in a given corporate credit union operation and determine the scope of the examination taking into consideration the many variables presented by the individual corporate credit union. When examiners determine a safety and soundness concern and/or a regulatory violation exists, they communicate with corporate credit union officials and staff to develop action steps to eliminate the concern(s).

Please be advised the CEG file size is approximately 1.5 MB, which will take you about 10 minutes to download using a 56k modem (i.e., if your modem speed is less than or greater than 56k it will take you more or less time).

If you have questions that are not addressed in this CEG, you may contact the OCCU at (703) 518-6640.